Mathematics Library

OCT 24 1949

Stacks

CANADIAN JOURNAL OF MATHEMATICS

Journal Canadien de Mathématiques

VOL. I - NO. 4

1949

Direct theorems on methods of summability	G. G. Lorentz	305
A generalization of Epstein zeta functions (with supplementary note by H. Weyl)	S. Minakshisundaram	320
Applications of combinatorial formulae to generalizations of Wilson's theorem	N. S. Mendelsohn	328
Axiomatic treatment of rank in infinite sets	R. Rado	337
Representation by quadratic forms	Gordon Pall	344
Graphs of degree three with a given abstract group	Robert Frucht	365
Factorization ladders and eigenfunctions	G. F. D. Duff	379
On a theorem of Liouville in fields of positive characteristic	K. Mahler	397

Published for

THE CANADIAN MATHEMATICAL CONGRESS

by the University of Toronto Press

EDITORIAL BOARD

H. S. M. Coxeter, A. Gauthier, L. Infeld, R. D. James, R. L. Jeffery, G. de B. Robinson

with the co-operation of

R. Brauer, J. Chapelon, D. B. DeLury, P. Dubreil, I. Halperin, W. V. D. Hodge, S. MacLane, L. J. Mordell, G. Pall, J. L. Synge, A. W. Tucker, W. J. Webber

The chief languages of the *Journal* are English and French.

Manuscripts for publication in the *Journal* should be sent to the *Editor-in-Chief*, H. S. M. Coxeter, University of Toronto. Every paper should contain an introduction summarizing the results as far as possible in such a way as to be understood by the non-expert.

All other correspondence should be addressed to the *Managing Editor*, G. de B. Robinson, University of Toronto.

The *Journal* is published quarterly. Subscriptions should be sent to the *Managing Editor*. The price per volume of four numbers is $6.00. This is reduced to $3.00 for individuals who are members of the following Societies:

Canadian Mathematical Congress
American Mathematical Society
Mathematical Association of America
London Mathematical Society
Société Mathématique de France

The Canadian Mathematical Congress gratefully acknowledges the assistance of the following towards the cost of publishing this Journal:

University of British Columbia
Ecole Polytechnique
McGill University
Queen's University
Loyola College
University of Manitoba
McMaster University
University of Toronto

and

The American Mathematical Society

AUTHORIZED AS SECOND CLASS MAIL, POST OFFICE DEPARTMENT, OTTAWA

DIRECT THEOREMS ON METHODS OF SUMMABILITY

G. G. LORENTZ

§ 1. Introduction

1.1. A regular Toeplitz method of summability is given by a transformation

$$\sigma_m = \sum_{n=0}^{\infty} a_{mn} s_n, \qquad m = 0, 1, 2, \ldots \tag{1.1(1)}$$

of the sequence s_n into the sequence σ_m. According to the definition of regularity, every such method sums a convergent sequence s_n to the value $\lim s_n$. The question naturally arises, whether there are more extensive classes of sequences summable by all regular methods 1.1(1) or at least by all such methods subject to some simple additional conditions. Questions of this kind have been treated by the author (Lorentz [2], [5]) and, from another point of view, by R. P. Agnew [2] [3] ; in this paper we wish to discuss the problem systematically.

We first define classes of sequences considered in the sequel. The *characteristic function* $\omega(n)$ of a (finite or infinite) sequence $n_1 < n_2 < \ldots$ of positive integers is defined for all $n \geqq 0$ as the number of n_ν satisfying the inequality $n_\nu \leqq n$. *Throughout the paper, $\Omega(n)$ denotes a non-decreasing positive function defined for $n \geqq 0$ and tending to $+\infty$ for $n \to +\infty$.* For any such function, the class $\mathfrak{C}_1(\Omega)$ consists of all real bounded sequences s_n for which the set of indices $n_1 < n_2 < \ldots$ with non-vanishing s_n has a characteristic function $\omega(n) \leqq \Omega(n)$. Again, the class $\mathfrak{C}_2(\Omega)$ is constituted of all real sequences s_n such that the sums $S_n = s_0 + \ldots + s_n$ have the property $S_n = O(\Omega(n))$.

$\Omega(n)$ is a *summability function of the first kind or of the second kind for the method A*, if all sequences of $\mathfrak{C}_1(\Omega)$ or $\mathfrak{C}_2(\Omega)$, respectively, are A-summable. Summability functions of the first kind (for brevity, we shall sometimes simply call them summability functions) have been introduced by the author (Lorentz [5]).

In § 2, we state some properties of summability functions, and give necessary and sufficient conditions for a function $\Omega(n)$ to be a summability function for a Toeplitz method A. § 3 deals with relations between summability functions and Tauberian conditions. § 4 introduces simple sufficient and simple necessary conditions used later. In § 5 we determine summability functions for several special methods; and Hausdorff methods are treated in § 6.

Received April 28, 1948.

§ 2. Summability Functions of the First and the Second Kind

2.1. First some remarks on characteristic functions. If the sequences n_ν, n'_ν have characteristic functions $\omega(n)$, $\omega'(n)$ respectively, then their sum has a characteristic function $\leqq \omega(n)+\omega'(n)$. Further, $n_\nu \leqq n'_\nu$ for all ν is equivalent to $\omega(n) \geqq \omega'(n)$, $n = 0, 1, \ldots$.

For every sequence n_ν with the characteristic function $\omega(n)$ and every positive integer k, a decomposition of n_ν into a sum of $k+1$ subsequences exists such that one sequence is finite and the others have characteristic functions $\leqq \omega(n)/k$. Indeed, the subsequences $n_1, n_2, \ldots, n_{k-1}$ and $\{n_{sk+i}\}$ $(s=1, 2, \ldots, i = 0, 1, \ldots, k-1)$ provide the required decomposition.

2.2. A summability function of the second kind for a method A is also a summability function of the first kind for A. If $\Omega(n)$ is a summability function and $\Omega'(n) \leqq C\Omega(n)$ for all $n \geqq 0$, C being a constant, then $\Omega'(n)$ is also a summability function of the same kind. The proof depends upon the decomposition of the sequence n_ν mentioned in **2.1.**

If the method A is contained in the method B, $A \subset B$, all summability functions of A are also summability functions of B.

For a summability function of the first kind $\Omega(n)$ we always may assume that

2.2(1) $$\Omega(n+1) - \Omega(n) \leqq 1, \qquad n \geqq 0.$$

For if $\Omega'(n)$ is defined by $\Omega'(x) = \Omega(0)$, $0 \leqq x < 1$ and, inductively, by $\Omega'(x) = \min [\Omega'(n-1)+1, \Omega(n)]$, $n \leqq x < n+1$, $n = 1, 2, \ldots$, then Ω' has the property 2.2(1) and is or is not a summability function together with Ω.

2.3. We proceed to formulate necessary and sufficient conditions in order that a given function $\Omega(n)$ be a summability function for a Toeplitz method 1.1(1).

Theorem 1. *$\Omega(n)$ is a summability function of the first kind for the method* 1.1(1), *if and only if*

2.3(1) $$\lim_{m\to\infty} \sum_{\nu=1}^{\infty} |a_{mn_\nu}| = 0$$

for every sequence n_ν with a characteristic function $\omega(n) \leqq \Omega(n)$, or if and only if

2.3(2) $$\lim_{m\to\infty} A(m;\Omega) = 0$$

where, for $m = 0, 1, \ldots$, $A(m;\Omega)$ is the least upper bound of $\sum_{\nu=1}^{\infty} |a_{mn_\nu}|$ for all sequences n_ν with $\omega(n) \leqq \Omega(n)$.

These conditions being fulfilled, every sequence $s_n \epsilon \mathfrak{C}_1(\Omega)$ is A-summable to 0.

For the proof, see Lorentz [5, theorems 9 and 10].

Theorem 2. *A function $\Omega(n)$ is a summability function of the second kind for a method* 1.1(1), *if and only if*

2.3(3) $$\lim_{m\to\infty} \sum_{n=0}^{\infty} \Omega(n) |a_{mn} - a_{m,n+1}| = 0.$$

If this condition is satisfied, every sequence $s_n \epsilon \mathfrak{C}_2(\Omega)$ is A-summable to 0.

Proof. First suppose that $\Omega(n)$ is a summability function of the second kind. Let ξ_n be any bounded sequence; put $S_n = \Omega(n)\xi_n$, $n = 0, 1, \ldots$; $S_{-1} = 0$ and $s_n = S_n - S_{n-1}$. Then

$$\sigma_m = \sum_{n=0}^{\infty} a_{mn} s_n = \sum_{n=0}^{\infty} a_{mn} [\Omega(n)\xi_n - \Omega(n-1)\xi_{n-1}]$$

is convergent and has a limit for $m \to \infty$. We choose $\xi_{2n} = \zeta_n$, $\xi_{2n+1} = 0$; σ_m becomes

$$\sigma_m = \sum_{n=0}^{\infty} \Omega(2n)\,(a_{m,2n} - a_{m,2n+1})\,\zeta_n = \Sigma b_{mn}\zeta_n.$$

This is a summability method applicable to all bounded sequences ζ_n. Since $b_{mn} \to 0$ for $m \to \infty$, $n = 0, 1, \ldots$, by a theorem of I. Schur [1] we have

$$\lim_{m\to\infty} \sum_{n=0}^{\infty} \Omega(2n)\,|a_{m,2n} - a_{m,2n+1}| = 0.$$

Odd indices $2n+1$ can be treated similarly; we thus obtain 2.3(3).

Conversely, if 2.3(3) holds, and if s_n is a sequence such that $S_n = O(\Omega(n))$, we have $a_{m,n+1}\Omega(n) \to 0$ for $n \to \infty$ and every fixed $m = 0, 1, \ldots$ and therefore $a_{m,n+1}S_n \to 0$. Letting n become infinite in the finite Abel transformation we have

$$\sigma_m = \sum_{n=0}^{\infty} a_{mn}s_n = \sum_{n=0}^{\infty} (a_{mn} - a_{m,n+1})\,S_n.$$

2.3(3) and $\lim_n a_{mn} = 0$ imply $\sigma_m \to 0$. This completes the proof.

2.4. A method A is called *strongly regular*, if every almost convergent sequence s_m is A-summable; the necessary and sufficient condition is (Lorentz [5]):

$$\text{2.4(1)} \qquad \lim_{m\to\infty} \sum_{n=0}^{\infty} |\,a_{mn} - a_{m,n+1}\,| = 0.$$

From this, one easily obtains:

THEOREM 3. *A regular Toeplitz method A is strongly regular if and only if A possesses a summability function of the second kind.*

The assertion follows at once from the criterion 2.4(1) and the following lemma:

LEMMA 1. *If $a_{mn} \geqq 0$ and if $\eta_m = \sum_{n=0}^{\infty} a_{mn} \to 0$, a function $\Omega(n)$ exists such that $\Sigma_n \Omega(n) a_{mn} \to 0$.*

Proof. For every $m = 0, 1, 2, \ldots$ there is clearly a function $\Omega_m(n)$ of the required kind for which $\Sigma_n \Omega_m(n) a_{mn} \leqq 2\eta_m$. Moreover, we can choose a non-decreasing sequence of positive integers $k_m \to +\infty$, for which $k_m\eta_m \to 0$. Let

$$\Omega(n) = \min_{m=0,1,\ldots} \{k_m + \Omega_m(n)\}, \qquad n = 0, 1, \ldots.$$

This function is non-decreasing, positive, and it is easy to see that $\Omega(n) \uparrow +\infty$. Finally, $\Sigma_n \Omega(n) a_{mn} \leqq k_m\eta_m + 2\eta_m \to 0$, which proves the lemma.

The analogue to Theorem 3 for summability functions of the first kind is this (Lorentz [5]): A Toeplitz method A possesses summability functions of the first kind, if and only if, for $m \to \infty$,

2.4(2) $$\max_{n=0,1,\dots} |a_{mn}| \to 0.$$

2.5. Another consequence of the lemma is

THEOREM 4. *For every summability function of the second kind $\Omega(n)$ for a method A there is another such function $\Omega_1(n)$ with $\Omega_1(n)/\Omega(n) \uparrow +\infty$.*

That generally not all summability functions of the second kind are of the form $\Omega(n) = o(\phi(n))$ with an appropriate $\phi(n)$ is shown by the example of Riemann's method R_2 in **5.4.**

A similar theorem is:

THEOREM 5. *For every summability function of the first kind $\Omega(n)$ for a method A there is another such function $\Omega_1(n)$ for which $\Omega_1(n)/\Omega(n) \uparrow +\infty$.*

Proof. Using the notation of Theorem 1 we have $A(m;\Omega) \to 0$. Moreover, by the theorem referred to above,

$$\delta_m = \max_n |a_{mn}| \to 0.$$

We choose a non-decreasing sequence of positive integers $k_m \uparrow +\infty$ such that

$$k_m A(m;\Omega) \to 0, \quad k_m \delta_m \to 0.$$

Then

2.5(1) $$A(m; k_m\Omega) \to 0.$$

For, according to **2.1**, every sequence of integers n_ν with the characteristic function $\leqq k_m\Omega(n)$ is a sum of a finite sequence consisting of k_m elements and of k_m infinite sequences whose characteristic functions are $\leqq \Omega(n)$. Therefore

$$\sum_\nu |a_{mn_\nu}| \leqq k_m\delta_m + k_m A(m;\Omega)$$

and 2.5(1) follows from the definition of $A(m; k_m\Omega)$.

We may choose integers $N_m \uparrow +\infty$ such that

$$\epsilon_m = \sum_{n>N_m} |a_{mn}| \to 0.$$

Now let

$$\Omega_1(n) = k_m\Omega(n), \qquad N_m \leqq n < N_{m+1},\ n = 1, 2, \dots,$$

then $\Omega_1(n)/\Omega(n) \uparrow +\infty$ and

$$A(m;\Omega_1) \leqq \epsilon_m + \sup_{\{n_\nu\}} \sum_{n_\nu \leqq N_m} |a_{mn_\nu}|,$$

where $\{n_\nu\}$ stands for all sequences whose characteristic functions are $\leqq \Omega_1(n)$. Since $\Omega_1(n) \leqq k_m\Omega(n)$ for $n \leqq N_m$,

$$A(m;\Omega_1) \leqq \epsilon_m + A(m; k_m\Omega).$$

This completes the proof.

§ 3. Relations between Summability Functions and Tauberian Conditions

3.1. A condition on a sequence s_n is called a *Tauberian condition* for a method A, if every sequence s_n, which is A-summable and satisfies this condition, is convergent. We now show, that the knowledge of summability functions of a method enables one to draw some conclusions about its Tauberian conditions.

Theorem 6. *If $\Omega(n)$ is a summability function (of the first kind) for a regular Toeplitz method A, then*

3.1(1) $$u_n = s_n - s_{n-1} = o(\Omega(n)^{-1})$$

is not a Tauberian condition for this method.

This theorem gives a precise limit from below for Tauberian conditions of the form $u_n = o(\phi(n))$ for all summability methods treated in §§ 5-6, except for the rather pathological method 5.3(3).

For the proof of Theorem 6 we need Lemma 2, interesting in itself. The following remarks are intended to elucidate its meaning. Both the conditions

3.1(2) $$u_n = O(n^{-\alpha}),\ \sigma_n = S_n/n = (s_0 + \ldots + s_n)/n = o(n^{\alpha-1})$$

constitute for every $0 \leqq \alpha \leqq 1$ a Tauberian condition for the method C_1 (Ananda Rau [1], Karamata [1], Boas, Jr. [1]). We show that the conditions 3.1(2) may not be relaxed: for every function $\Omega(n)$ for which $\Sigma\Omega(n)^{-1} = +\infty$ there is a divergent series Σu_n such that $u_n = O(\Omega(n)^{-1})$, $\sigma_n = O(\Omega(n)/n)$. Even more is true:

Lemma 2. *For every function $\Omega(n)$ for which $\Sigma\Omega(n)^{-1} = +\infty$ a bounded divergent sequence s_n exists such that $u_n = s_n - s_{n-1} = O(\Omega(n)^{-1})$ and that the characteristic function of the indices n which have the property $s_n \neq 0$ does not exceed $\Omega(n)$.*

Proof. We define two sequences of positive integers $m_1 < n_1 < \ldots < m_\nu < n_\nu < \ldots$ such that $\Omega(m_1)^{-1} < 1/9$, that the characteristic function of the sum of the intervals $m_\nu \leqq n \leqq n_\nu$, $\nu = 1, 2, \ldots$ is $\leqq \Omega(n)$ and that furthermore

3.1(3) $$\sum_{m_\nu \leqq n \leqq n_\nu} \Omega(n)^{-1} \geqq 1/3, \qquad \nu = 1, 2, \ldots.$$

We proceed by induction. Let $m_1, n_1, \ldots, m_{\nu-1}, n_{\nu-1}$ be already defined. Then m_ν is chosen such that

$$\sum_{\mu=1}^{\nu-1} (n_\mu - m_\mu + 1) \leqq \Omega(m_\nu)/2 \leqq \Omega(n)/2, \qquad n \geqq m_\nu.$$

Since $\Omega(m_\nu) \geqq 4$, the integer $N = m_\nu + 1$ has the property that the characteristic function of the interval $m_\nu \leqq n \leqq N$ does not exceed $\Omega(n)/2$ for $n \geqq m_\nu$. If all integers $N \geqq m_\nu + 1$ have this property, n_ν is chosen arbitrarily to satisfy 3.1(3). On the other hand, if N_0 is the first integer $> m_\nu + 1$ lacking the

above property, we put $n_\nu = N_0 - 1$. Then $N_0 - m_\nu + 1 \geqq \Omega(N_0)/2$. Hence

$$\sum_{m_\nu \leqq n \leqq N_0} \Omega(n)^{-1} \geqq (N_0 - m_\nu + 1)\Omega(N_0)^{-1} \geqq \frac{1}{2}.$$

In this case 3.1(3) also holds.—The sum of the intervals $m_\nu \leqq n \leqq n_\nu$, $\nu = 1, 2, \ldots$ thus defined has a characteristic function $\leqq \Omega(n)$.

We now choose integers l_ν, $\nu = 1, 2, \ldots$ for which $m_\nu \leqq l_\nu < n_\nu$ and

$$\sum_{m_\nu \leqq n \leqq l_\nu} \Omega(n)^{-1} \geqq \frac{1}{9}, \quad \sum_{l_\nu < n \leqq n_\nu} \Omega(n)^{-1} \geqq \frac{1}{9}, \qquad \nu = 1, 2, \ldots$$

Then for $m_\nu \leqq n \leqq n_\nu$, $\nu = 1, 2, \ldots$ real u_n exist such that $|u_n| \leqq \Omega(n)^{-1}$, $u_n \geqq 0$ for $m_\nu \leqq n \leqq l_\nu$, $u_n \leqq 0$ for $l_\nu < n \leqq n_\nu$, and

$$\sum_{m_\nu \leqq n \leqq l_\nu} u_n = \frac{1}{9}, \quad \sum_{l_\nu < n \leqq n_\nu} u_n = -\frac{1}{9}.$$

Let $u_n = 0$ for all remaining n. It is easily seen that the sequence $s_n = \sum_0^n u_\nu$ has all the required properties.

Proof of Theorem 6. For a summability function $\Omega(n)$ of a regular Toeplitz method we have $\Sigma\Omega(n)^{-1} = +\infty$. For otherwise $n\Omega(n)^{-1} \to 0$, and so $n = o(\Omega(n))$ would be a summability function. Thus all bounded sequences are A-summable to 0, which contradicts the theorem of I. Schur referred to in **2.3.** Thus by Lemma 2, we obtain the assertion of Theorem 6 with the condition $u_n = O(\Omega(n)^{-1})$ instead of 3.1(1). The general statement now follows from Theorem 5.

§ 4. Summability Functions of the Form $\Omega(n) = o(n)$

4.1. Before treating special methods we insert a few simple sufficient and simple necessary conditions for summability functions. In many cases they are all contained in the formula $\Omega(n) = o(n)$.

Theorem 7. *Suppose that there is a monotone majorant* (a_{mn}) *of the matrix* (a_{mn}) *having the properties:* $a_{mn} \geqq 0$, a_{mn} *is non-increasing for every fixed* $m = 0, 1, \ldots$, $a_{m0} \to 0$, $|a_{mn}| \leqq a_{mn}$ *and finally*

$$4.1(1) \qquad \sum_{n=0}^{\infty} a_{mn} \leqq M, \qquad m = 0, 1, \ldots$$

with a constant M. *Then all functions* $\Omega(n) = o(n)$ *are summability functions for the method* 1.1(1).

Proof. It will be sufficient to prove

$$4.1(2) \qquad \lim_{m \to \infty} \sum_{\nu=1}^{\infty} a_{mn_\nu} = 0$$

for every sequence n_ν with a characteristic function $\omega(n) = o(n)$. Let p be an arbitrary positive integer; we may assume (by omitting, if necessary, a finite number of n_ν), that $\omega(n) \leqq n/p$ holds for all $n = 0, 1, \ldots$. Since $n_\nu \geqq p\omega(n_\nu)$

$= \nu p$, it is possible, by induction in k, to determine integers n_ν^k, $\nu = 1, 2, \ldots,$ $k = 1, 2, \ldots, p$, all of which are different, such that $n_\nu^k \leqq n_\nu$. Then

$$p \sum_{\mu=1}^{\nu} a_{m,n_\mu} \leqq \sum_{\mu \leqq \nu} a_{m,n_\mu^k} \leqq M.$$

Hence $\Sigma_\nu a_{mn_\nu} \leqq M/p$. Since p was arbitrary, our result is established.

Summability functions other than those of the form $o(n)$ may occur in abnormal cases only, as is shown by the following theorem:

THEOREM 8. *If a Toeplitz method A possesses a summability function $\Omega(n) \neq o(n)$, then A is a gap method, that is to every $\epsilon > 0$ and every $C > 0$ there is a corresponding n' as large as we please such that*

4.1(3) $$\sum_{n' \leqq n \leqq Cn'} |a_{mn}| < \epsilon, \qquad m = 0, 1, \ldots.$$

Proof. Suppose that $\overline{\lim}\, \Omega(n)/n > 2c > 0$. Let $\epsilon > 0$ and $C > 0$ be chosen arbitrarily; we may assume that C/c is an integer. According to 2.3(2), an m_0 exists such that

4.1(4) $$A(m; \Omega) < \epsilon c/C, \qquad m \geqq m_0.$$

For an n_0 sufficiently large we have

4.1(5) $$\sum_{n=n_0}^{\infty} |a_{mn}| < \epsilon, \qquad m \leqq m_0.$$

Let an integer n' be chosen for which $n' \geqq n_0$, $cn' \geqq 1$ and $\Omega(n')/n' \geqq 2c$. Each of the closed intervals

$$[n', n' + cn'], [n' + cn', n' + 2cn'], \ldots, \left[n' + \left(\frac{C}{c} - 1\right)cn', n' + Cn'\right]$$

contains no more than

$$cn' + 1 \leqq 2cn' \leqq \Omega(n')$$

integers; characteristic functions of each interval are therefore $\leqq \Omega(n)$ for $n = 0, 1, \ldots$. By 4.1(4),

$$\sum_{n' \leqq n \leqq Cn'} |a_{mn}| \leqq \frac{C}{c} A(m; \Omega) < \epsilon, \qquad m \geqq m_0.$$

The same inequality for $m \leqq m_0$ follows from 4.1(5).

The following remarks are useful for the determination of summability functions of the second kind. Let σ_n signify the Cesàro mean $\sigma_n = (s_0 + \ldots + s_n)/(n+1)$ of a sequence s_n. From the definition 1.1 it follows that all functions $\Omega(n) = o(\phi(n))$ are summability functions of the second kind of a method A if and only if $\sigma_n - s = o(\phi(n)n^{-1})$ implies the A-summability of the sequence s_n to 0. Thus, the assertion, that all functions $\Omega(n) = o(n)$ have this property for A is equivalent to $A \supset C_1$. Suppose, for instance, that $a_{mn} \geqq 0$ for all m, n and that for every fixed m the a_{mn} are first increasing up to their maximal value for $n = n_0 = n_0(m)$ and then decreasing to 0. Then $A \supset C_1$ holds if and only if

4.1(6) $$n_0 a_{mn_0} \leqq M$$

is true with an M independent of m. For 4.1(6) is clearly equivalent to

4.1(7) $$\sum_{n=0}^{\infty} n\,|a_{mn} - a_{m,n+1}| \leqq M'$$

which is necessary and sufficient for the inclusion $A \supset C_1$ for any regular Toeplitz method A (Orlicz [1]).

§ 5. Some Special Methods

5.1. The methods of Cesàro and Abel. All summability functions of the method C_1 are clearly given by the formula $\Omega(n) = o(n)$. The same is true for $C_\alpha(\alpha > 0)$ and the Abel method A, since all these methods are equivalent for bounded sequences. All functions $\Omega(n) = o(n)$ are also summability functions of the second kind for the methods $C_\alpha(\alpha \geqq 1)$ and A, since these methods contain C_1. There are no other functions, for A is not a gap method as is seen from

$$(1-r)\sum_{\nu=n}^{2n-1} r^\nu = r^n(1-r^n) \to e^{-1} - e^{-2}$$

for $r = 1 - n^{-1}$, $n \to \infty$.

Finally, by a simple computation it may be deduced from Theorem 2 that all summability functions of the second kind for $C_\alpha(0 < \alpha < 1)$ are furnished by the formula $\Omega(n) = o(n^\alpha)$.

5.2. The methods of Euler and Borel. The Euler method $E_t(0 < t < 1)$ is defined by the transformation

5.2(1) $$\sigma_n = \sum_{\nu=0}^{n} p_\nu(t) s_\nu,$$

$$p_\nu(t) = p_{\nu n}(t) = \binom{n}{\nu} t^\nu (1-t)^{n-\nu},\ 0 \leqq \nu \leqq n,\ p_{n+1,n}(t) = 0,$$

and the Borel method by

5.2(2) $$\sigma(x) = e^{-x} \sum_{n=0}^{\infty} \frac{x^n}{n!} s_n, \qquad x \to +\infty.$$

For these methods a function $\Omega(n)$ is a summability function of the first or of the second kind if and only if $\Omega(n) = o(\sqrt{n})$. Since $E_t \subset B$, it will be sufficient to prove: (i) Every function $\Omega(n) = o(\sqrt{n})$ is a summability function of the second kind for $E_t(0 < t < 1)$; (ii) If $\Omega(n) \neq o(\sqrt{n})$, $\Omega(n)$ is not a summability function for B.

To prove (i) observe that the sum 2.3(3) takes for the transformation 5.2(1) the form

$$\Delta(n;\Omega) = \sum_{\nu=0}^{n} \Omega(\nu)\,|p_\nu(t) - p_{\nu+1}(t)| \leqq \Omega(n) \sum_{\nu=0}^{n} |p_\nu(t) - p_{\nu+1}(t)|$$

$$\leqq 2\Omega(n) \max_{0 \leqq \nu \leqq n} p_\nu(t) \leqq 2Cn^{-\frac{1}{2}}\Omega(n) \to 0,$$

if $\Omega(n) = o(\sqrt{n})$. As a matter of fact the "Newtonian probability" $p_{\nu n}(t)$ for

fixed n, t and ν varying in the interval $0 \leqq \nu \leqq n$ increases first and then decreases; and the maximal value of $p_\nu(t)$ does not exceed $Cn^{-\frac{1}{2}}$, where C depends on t only.

(ii) Let $\Omega(n) \neq o(\sqrt{n})$, then a $\delta > 0$ exists for which $\Omega(n) \geqq \delta\sqrt{n}$ holds for an infinity of n. For these n and the Borel transformation 5.2(2)

$$A(n;\Omega) \geqq e^{-n} \sum_{n<\nu\leqq n+\delta\sqrt{n}} n^\nu/\Gamma(\nu+1) \geqq C_1 e^{-n}\Sigma n^\nu \nu^{-(\nu+\frac{1}{2})} e^\nu$$

$$= C_1 \sum_{n<\nu\leqq n+\delta\sqrt{n}} \nu^{-\frac{1}{2}} \left(1 - \frac{\nu-n}{\nu}\right)^\nu e^{\nu-n}.$$

(C_1, C_2, ... are constants). Since $\nu \log\left(1 - \frac{\nu-n}{\nu}\right) \geqq -(\nu-n) + C_2$ for $0 \leqq \nu - n \leqq \delta\sqrt{n}$,

$$A(n;\Omega) \geqq C_3 \sum_{n<\nu\leqq n+\delta\sqrt{n}} \nu^{-\frac{1}{2}} \geqq C_4 > 0.$$

Hence, by 2.3(2), $\Omega(n)$ is not a summability function for the method B.

5.3. Some other methods. For the Lambert method L

$$\sigma(x) = \sum_{\nu=1}^{\infty} \frac{\nu(1-x)}{1-x^\nu} u_\nu = \sum_{\nu=1}^{\infty} a_\nu(x) s_\nu, \qquad x \to 1-,$$

5.3(1)

$$a_\nu(x) = \frac{x^\nu(\nu - x - \cdots - x^\nu)}{(1+\cdots+x^{\nu-1})(1+\cdots+x^\nu)}$$

(both forms are equivalent, see for instance Lorentz [3, theorem 10]) and for the method

5.3(2) $$\sigma_n = \sum_{\nu=0}^{n} \binom{n}{\nu} \frac{\nu!}{n^\nu} u_\nu = s_0 + \sum_{\nu=1}^{n} \left(1 - \frac{1}{n}\right) \cdots \left(1 - \frac{\nu-1}{n}\right) \frac{\nu}{n} s_\nu$$

(Rey-Pastor [1], S. Bernstein [1], Amerio [1]) all summability functions of the first and of the second kind and only these are furnished by $\Omega(n) = o(n)$. The positive part follows from 4.1(6) with $n_0 = 0$ for L and with $n_0 \cong \sqrt{n}$ for the method 5.3(2); and the negative part is a consequence of Theorem 8. We leave details to the reader.

The method

5.3(3) $$\sigma_m = s_{2^m}$$

has no summability functions at all; but Tauberian theorems exist for this method. Thus, $u_n = o(n^{-1})$ is a Tauberian condition (o may not be replaced by O).

5.4. The Riemann methods R_k. R_k, $k = 2, 3, \ldots$ is related to the transformation

$$\sigma(x) = \sum_{n=0}^{\infty} \left(\frac{\sin nx}{nx}\right)^k u_n$$

5.4(1)

$$= \sum_{n=0}^{\infty} \left\{ \left(\frac{\sin nx}{nx}\right)^k - \left(\frac{\sin (n+1)x}{(n+1)x}\right)^k \right\} s_n, \qquad x \to 0+.$$

Both forms are equivalent for bounded s_n. We take the second as the definition.

The derivative of the function $\phi(u) = (\sin u/u)^k$ has the property $|\phi'(u)| \leqq C(u+1)^{-k}$, C depending only on k. Hence for $x > 0$

$$\left|\frac{d}{du}\,\phi(xu)\right| = |\,\phi'(xu)\,|\,x \leqq Cx(xu+1)^{-k} \leqq C_1 x s^{-k} \text{ for } u \geqq \frac{s\pi}{x},\ s = 1, 2, \ldots.$$

We put $a_n(x) = (\sin nx/nx)^k - (\sin (n+1)x/(n+1)x)^k$ and

$$\alpha_0(x) = C_1 x, \quad \alpha_n(x) = C_1 x s^{-k} \text{ for } \frac{s\pi}{x} \leqq n < \frac{(s+1)\,\pi}{x}.$$

The functions $\alpha_n(x)$ constitute a monotone majorant for $a_n(x)$ in the sense of Theorem 7. In particular,

$$\sum_{n=0}^{\infty} \alpha_n(x) \leqq \frac{C_2}{x}\, x \left(1 + \sum_{s=1}^{\infty} s^{-k}\right) = M < +\infty.$$

By Theorem 7 (or rather by its continuous analogue), all functions $\Omega(n) = o(n)$ are summability functions for the methods R_k, $k = 2, 3, \ldots$. There are no others by Theorem 8, since

$$\sum_{\frac{\pi}{x} \leqq n < \frac{2\pi}{x}} |\,a_n(x)\,|$$

converges for $x \to 0+$ to the positive number $\max |\phi(u)|$, $\pi \leqq u \leqq 2\pi$.

Summability functions of the second kind are also given by $\Omega(n) = o(n)$, if $k = 3, 4, \ldots$. As to R_2, they are defined by

5.4(2)
$$\sum_{n=1}^{\infty} \Omega(n) n^{-2} < +\infty.$$

For consider

$$\Delta(x; \Omega) = \sum_{n=0}^{\infty} \Omega(n)\,|\,a_n(x) - a_{n+1}(x)\,|$$

5.4(3)
$$= \sum_{n=0}^{\infty} \Omega(n)\,|\,\phi(nx) - 2\phi(nx+x) + \phi(nx+2x)\,|\,.$$

The derivative $\phi''(u)$ exists for $u \geqq 0$ and has the properties $|\phi''(u)| \leqq C_3 u^{-k}$, $|\phi''(u)| \leqq C_4$. Therefore $(0 < \theta < 1)$

$$|\Delta^2\phi(nx)| = x^2|\phi''(nx + 2\theta x)| \leqq C_4 x^2, \qquad 0 \leqq nx \leqq 1,$$
$$|\Delta^2\phi(nx)| \leqq C_3(nx)^{-k}x^2, \qquad nx \geqq 1.$$

Thus, 5.4(3) becomes

$$\Delta(x;\Omega) = \sum_{nx<1} + \sum_{nx\geqq 1}$$
$$\leqq C_4 x^2 \sum_{nx<1} \Omega(n) + C_3 x^{2-k} \sum_{nx\geqq 1} \Omega(n) n^{-k}.$$

Since $\Omega(n) = o(n)$ also holds in case of 5.4(2), the first term on the right is $= C_4 x^2 o(\Sigma_{n<x^{-1}} n) = C_4 x^2 o(x^{-2}) = o(1)$, while the second term $= C_3 x^{2-k} o(\Sigma_{n\geqq x^{-1}} n^{1-k}) = C_3 x^{2-k} o(x^{k-2}) = o(1)$ for $k \geqq 3$ and $= C_3 o(1)$ for $k = 2$, if 5.4(2) is fulfilled. It remains to show that, if $\Sigma\Omega(n)n^{-2} = +\infty$, $\Omega(n)$ is not a summability function of the second kind for R_2.

For small $x > 0$, we wish to estimate $|\Delta^2\phi(nx)| = x^2|\phi''(u)|$, $u = nx + 2\theta x$, $0 < \theta < 1$ from below for $\left|n - \frac{s\pi}{x}\right| \leqq \pi/10x$. Since $\phi''(u) = 2u^{-2}\cos 2u + O(u^{-3})$, if $u \to \infty$, $|\phi''(u)| \geqq u^{-2}$ holds for $|u - s\pi| \leqq \pi/8$ and all sufficiently large integers s. Thus $|\Delta^2\phi(nx)| \geqq n^{-2}$ for $\left|n - \frac{s\pi}{x}\right| \leqq \pi/10x$. Since

$$\sum_{\left|n-\frac{s\pi}{x}\right| \leqq \frac{\pi}{10x}} \Omega(n)|\Delta^2\phi(nx)| \geqq \sum_{\left|n-\frac{s\pi}{x}\right| \leqq \frac{\pi}{10x}} \Omega(n)n^{-2}$$
$$\geqq C_5 \sum_{\frac{(s-1)\pi}{x} + \frac{\pi}{10x} \leqq n \leqq \frac{s\pi}{x} + \frac{\pi}{10x}} \Omega(n)n^{-2} = v_s$$

and since the series Σv_s is divergent, $\Delta(x;\Omega) = \sum_{n=0}^{\infty}\Omega(n)\,|\,\Delta^2\phi(nx)\,| = +\infty$, which proves our result.

§ 6. Hausdorff Methods

6.1. A Hausdorff method H_g is defined by the transformation

$$6.1(1) \qquad \sigma_n = \sum_{\nu=0}^{n} a_{n\nu}s_\nu = \int_0^1 \sum_{\nu=0}^{n} p_{\nu n}(x)s_\nu\, dg(x);$$

$g(x)$ is a function of bounded variation in $[0, 1]$ and $p_{\nu n}(x) = p_\nu(x)$ is the "Newtonian probability" $\binom{n}{\nu}x^\nu(1-x)^{n-\nu}$. Without loss of generality we may assume, that $g(x)$ is normalized, that is, it has the properties $g(0) = 0$ and $g(x) = [g(x+) + g(x-)]/2$ for $0 < x < 1$.

H_g is regular if and only if $g(x)$ is continuous at $x = 0$ and if $g(1) = 1$. H_g is strongly regular if, and only if, H_g possesses summability functions of the *first* kind or, if and only if, $g(x)$ is continuous at $x = 1$ (Lorentz [5]). In this section we determine the summability functions for a method H_g in terms of

the generating function $g(x)$. The following theorem yields summability functions for every method H_g with a discontinuous $g(x)$.

THEOREM 9. (i) *A regular Hausdorff method can not be a gap method.* (ii) *If H_g is strongly regular, all functions $\Omega(n) = o(\sqrt{n})$ are summability functions for H_g.* (iii) *If $g(x)$ has a jump at a point $0 < x_0 < 1$, then all summability functions of H_g are of the form $\Omega(n) = o(\sqrt{n})$.*

To prove (i), suppose that $g(x)$ is continuous at $x = 0$; let $0 < a < b < 1$ be two points of continuity of $g(x)$. We choose a q, $0 < q < 1$, arbitrarily. If H_g is a gap method, then, for every $\epsilon > 0$,

$$\sum_{N \leqq \nu \leqq bN/aq} |a_{n\nu}| < \epsilon, \qquad n = 0, 1, \ldots$$

is true for some N as large as we please. To every sufficiently large N there corresponds an integer $n = n(N)$ such that $nq < N/a < n$. Then $a < \nu/n < b$ implies $N \leqq \nu \leqq bN/aq$. Hence

$$\left| \int_0^1 \sum_{a \leqq \frac{\nu}{n} \leqq b} p_{\nu n}(x) dg(x) \right| \leqq \sum_{a \leqq \frac{\nu}{n} \leqq b} |a_{n\nu}| < \epsilon.$$

The sum under the integral converges to 1, if $a < x < b$ and to 0 outside of this interval. Letting n become infinite, we obtain

$$\left| \int_a^b dg(x) \right| \leqq \epsilon.$$

Since ϵ was arbitrary, $g(a) = g(b)$. Therefore, the normalized function $g(x)$ is $= 0$ in $0 \leqq x < 1$. As $g(1) = 1$, 6.1(1) becomes $\sigma_n = s_n$, which contradicts the assumption that H_g is a gap method.

(ii) Suppose that H_g is strongly regular, that $\Omega(n) = o(\sqrt{n})$ and that ν_k is a sequence with a characteristic function $\omega(n) \leqq \Omega(n)$. We put

$$6.1(2) \qquad f_n(x) = \sum_{\nu_k \leqq n} p_{\nu_k n}(x).$$

Then $f_n(x) \to 0$ uniformly in $\delta \leqq x \leqq 1 - \delta$ for any fixed $\delta > 0$. For in this interval the estimate $p_{\nu n}(x) \leqq Cn^{-\frac{1}{2}}$ holds with a constant C depending only on δ. Therefore $0 \leqq f_n(x) \leqq Cn^{-\frac{1}{2}}\omega(n) = o(1)$. We are now in a position to prove that 2.3(1) holds, that is that $\Omega(n)$ is a summability function. If $V(x) = \operatorname{var} g(t)$ in $0 \leqq t \leqq x$,

$$\sum_{\nu_k \leqq n} |a_{n\nu_k}| \leqq \int_0^1 f_n(x) dV(x) = \int_0^\delta + \int_\delta^{1-\delta} + \int_{1-\delta}^1.$$

The second integral converges to zero as $n \to \infty$, and the remaining two are arbitrarily small with δ, since $0 \leqq f_n \leqq 1$ and $V(x)$ is continuous at $x = 0$ and $x = 1$.

It remains to prove (iii). Let α be the jump of $g(x)$ at $x = x_0$, and suppose $\Omega(n)n^{-\frac{1}{2}} \not\to 0$. We can choose a $\delta > 0$ such that for an infinity of n

$$\Omega(x_0 n/2)n^{-\frac{1}{2}} \geqq \delta. \tag{6.1(3)}$$

We wish to show that $A(n;\Omega) \not\to 0$ (compare 2.3(2)). If n is an integer satisfying 6.1(3), let ν_k be the finite sequence consisting of all ν with the property $|\nu/n - x_0| < \delta/2n^{\frac{1}{2}}$. We need the following result concerning the probability $p_{\nu n}$: an absolute constant C_1 and a $C_2 = C_2(x_0, \delta) > 0$ exist such that

$$\begin{cases} \sum\limits_{|\nu/n - x| \geqq n^{-\frac{1}{2}}} p_{\nu n}(x) \leqq C_1 n^{-2}, \\ \sum\limits_{|\nu/n - x_0| < \delta/2n^{\frac{1}{2}}} p_{\nu n}(x) \geqq C_2. \end{cases} \tag{6.1(4)}$$

We have

$$A(n;\Omega) = \sum_k \left| \int_0^1 p_{\nu_k n}(x)dg(x) \right|$$

$$\geqq |\alpha| \sum_k p_{\nu_k n}(x_0) - \int_0^1 \sum_k p_{\nu_k n}(x)dV(x),$$

where $V(x)$ is the variation of the function $g^*(x)$, resulting from $g(x)$ by omission of the jump α. The latter integral is smaller than

$$\operatorname*{var}_{\left|\frac{\nu}{n} - x\right| \leqq n^{-\frac{1}{2}}} g^*(x) + \operatorname*{var}_{0 \leqq x \leqq 1} g^*(x) \cdot C_1 n^{-2} \to 0, \qquad n \to \infty.$$

Thus by 6.1(3) and the second part of 6.1(4), $A(n;\Omega) \not\to 0$, and the proof of the theorem is complete.

6.2. We now treat methods H_g for which the generating function $g(x)$ is absolutely continuous.

THEOREM 10. *If $g(x)$ is absolutely continuous, then the summability functions for the method H_g are furnished by the formula $\Omega(n) = o(n)$.*

Proof. That there are no summability functions which do not satisfy $\Omega(n) = o(n)$ is implied by Theorems 8 and 9(i). Suppose now that ν_k is any sequence of integers with a characteristic function $\omega(n) = o(n)$. If $f_n(x)$ is again defined by 6.1(2),

$$\int_0^1 f_n(x)dx = \sum_k \int_0^1 p_{\nu_k}(x)dx = \frac{1}{n+1}\,\omega(n) \to 0.$$

Therefore, for every $\epsilon > 0$ and every integer n sufficiently large, the interval $[0.\ 1]$ may be represented as the sum $e_n + e_n'$ of two disjoint measurable sets e_n, e_n' for which $me_n < \epsilon$ and $f_n(x) < \epsilon$ if $x \in e_n'$. Hence

$$\sum_k |a_{n\nu_k}| \leqq \sum_k \int_0^1 p_{\nu_k}(x)\,|g'(x)|\,dx = \int_0^1 f_n(x)\,|g'(x)|\,dx$$

$$= \int_{e_n} + \int_{e_n'} \leqq \int_{e_n} |g'|\,dx + \epsilon \int_0^1 |g'|\,dx.$$

Since both the last terms are arbitrarily small with ϵ, the proof is complete.

By combining a gap theorem of Agnew [1] with a result of the author (Lorentz [4, theorem 1]), one may deduce that

6.2(1) $$u_n = o\left(\frac{1}{n}\right)$$

is a Tauberian condition for any Hausdorff method. Theorems 6 and 10 show now that $u_n = o(\phi(n))$ is not a Tauberian condition for any Hausdorff method with an absolutely continuous $g(x)$ if $\phi(n) \downarrow 0$ and $n\phi(n) \to +\infty$.

As to the summability functions of the second kind, we are able to show that all functions $\Omega(n) = o(\sqrt{n})$ are summability functions of the second kind for the method H_g if $g(x) \in$ Lip 1. We do not know whether this result can be improved.

Suppose $\Omega(n) = o(\sqrt{n})$; we shall show that

$$\Delta(n;\Omega) = \sum_{\nu=0}^{n} \Omega(\nu) \left| \int_0^1 \{ p_\nu(x) - p_{\nu+1}(x) \}\, dg(x) \right| \to 0.$$

Since $g'(x)$ is bounded, it will be sufficient to prove

6.2(2) $$\begin{aligned} \bar{\Delta}(n) &= \Omega(n) \int_0^1 \sum_{\nu=0}^{n} \left| p_\nu(x) - p_{\nu+1}(x) \right| dx \\ &= 2\Omega(n) \int_0^1 \max_{0 \le \nu \le n} p_\nu(x)\, dx \to 0. \end{aligned}$$

For a fixed x, the above maximum is attained for a $\nu = \nu_0(x)$ such that $\left| \nu_0/n - x \right| < n^{-1}$. We use the estimate (Lorentz [1])

6.2(3) $p_{\nu n}(x) \le [x(1-x)n]^{-\frac{1}{2}}$, if $\left| \nu/n - x \right| < x/10$, $\left| \nu/n - x \right| < (1-x)/10$.

Hence,

$$p_{\nu_0 n}(x) \le [x(1-x)n]^{-\frac{1}{2}}, \qquad 10/n \le x \le (n-10)/n.$$

Therefore

$$\begin{aligned} \bar{\Delta}(n) &= 2\Omega(n) \left\{ \int_{10/n}^{(n-10)/n} + \int_0^{10/n} + \int_{(n-10)/n}^1 \right\} \\ &\le 2\Omega(n) \left\{ \int_0^1 \frac{dx}{\sqrt{x(1-x)n}} + \frac{20}{n} \right\} = o(1), \end{aligned}$$

which proves 6.2(2).

References

R. P. Agnew, [1] "Analytic extension by Hausdorff methods," *Trans. Amer. Math. Soc.*, vol. 52 (1942), 217-237.

——— [2] "Convergence fields of methods of summability," *Ann. of Math.*, vol. (2) 46 (1945), 93-101.

——— [3] "A simple sufficient condition that a method of summability be stronger than convergence," *Bull. Amer. Math. Soc.*, vol. 52 (1946), 128-132.

L. Amerio, [1] "Un metodo di sommazione per le serie di potenze," *Ann. Scuola norm. sup., Pisa, Sci. fis. mat.*, vol. (2) 8 (1939), 167-180.

S. Bernstein, [1] "Sur la convergence de certaines suites des polynomes," *J. Math. Pures Appl.*, vol. (9) 15 (1935), 345-358.

R. P. Boas, Jr., [1] "Tauberian theorems for $(C, 1)$ summability," *Duke Math. J.*, vol. 4 (1938), 227-230.

J. Karamata, [1] "Eine weitere Umkehrung des Cesàroschen Limitierungsverfahrens," *Glas Srpske Akad.*, vol. 163 (80) (1935), 59-70.

G. G. Lorentz, [1] "Zur Theorie der Polynome von S. Bernstein," *Rec. Math.*, n.s. vol. 2 (1937), 543-556.

——— [2] "Beziehungen zwischen den Umkehrsätzen der Limitierungstheorie," *Bericht der Math. Tagung, Tübingen*, (1946), 97-99.

——— [3] "Über Limitierungsverfahren, die von einem Stieltjes-Integral abhängen," *Acta Math.*, vol. 79 (1947), 255-272.

——— [4] "Tauberian theorems and Tauberian conditions," *Trans. Amer. Math. Soc.*, vol. 63 (1948), 226-234.

——— [5] "A contribution to the theory of divergent series," *Acta Math.*, vol. 80 (1948), 167-190.

W. Orlicz, [1] "Zur allgemeinen Limitierungstheorie," *Tôhoku Math. J.*, vol. 26 (1926), 233-237.

K. Ananda Rau, [1] "On the convergence and summability of Dirichlet's series," *Proc. London Math. Soc.* IIs., vol. 34 (1932), 414-440.

J. Rey-Pastor, [1] "Un método de sumacion de series," *Rend. Circ. Mat. Palermo*, vol. 55 (1931), 450-455.

I. Schur, [1] "Über lineare Transformationen in der Theorie der unendlichen Reihen," *J. Reine Angew. Math.*, vol. 151 (1921), 79-111.

University of Toronto

A GENERALIZATION OF EPSTEIN ZETA FUNCTIONS

S. MINAKSHISUNDARAM

(*With a supplementary note by* HERMANN WEYL)

§ 1. An Epstein zeta function (in its simplest form) is a function represented by the Dirichlet's series

$$\sum{}' \frac{\exp i\,(n_1a_1+\cdots+n_ka_k)}{(n_1^2+n_2^2+\cdots+n_k^2)^s}, \qquad s=\sigma+i\tau \tag{1}$$

where $a_1 \ldots a_k$ are real and $n_1, n_2, \ldots n_k$ run through integral values. The properties of this function are well known and the simplest of them were proved by Epstein [2, 3]. The aim of this note is to define a general class of Dirichlet's series, of which the above can be viewed as an instance, and to discuss the problem of analytic continuation of such series.

The point of view is the following: The exponential functions $\exp i(n_1x_1 + \cdots + n_kx_k)$ may be viewed as the eigenfunctions of

$$\Delta u + \lambda u \equiv \sum_{i=1}^{k} \frac{\partial^2 u}{\partial x_i^2} + \lambda u = 0 \tag{2}$$

in the domain $D \equiv (0 \leq x_1, \ldots, x_k \leq 2\pi)$, the boundary condition being

$$\begin{aligned} &u(0, x_2, \ldots, x_k) = u(2\pi, x_2, \ldots, x_k) \\ &u(x_1, 0, x_3, \ldots, x_k) = u(x_1, 2\pi, x_3, \ldots, x_k) \\ &\quad\cdots \qquad\qquad\qquad\qquad \cdots \\ &u(x_1, \ldots, x_{k-1}, 0) = u(x_1, \ldots, x_{k-1}, 2\pi). \end{aligned} \tag{3}$$

The associated eigenvalues may be verified to be $n_1^2+\ldots+n_k^2$. If we arrange the eigenfunctions and eigenvalues into sequences $\omega_n(x)$, λ_n we observe that (1) may be written as

$$\sum{}' \frac{\omega_n(x)\overline{\omega_n(y)}}{\lambda_n{}^s}, \qquad x = (x_1, \ldots, x_k)$$

(we have only to set $a_i = x_i - y_i$ in (1)), where Σ' indicates that the zero eigenvalue is omitted in the summation.

Taking this point of view, we shall consider the eigenfunctions of (2) for a general class of domains and for the I and II boundary value problems and study the corresponding Dirichlet's series which may be easily defined.

Received July 8, 1948.

§ 2. In the k-dimensional Euclidean space, let D denote a bounded domain with a regular boundary B, so that the following boundary value problem

$$\Delta u + \lambda u \equiv \sum_{i=1}^{k} \frac{\partial^2 u}{\partial x_i^2} + \lambda u = 0, \tag{4}$$

$$u(x) \equiv u(x_1, \ldots, x_k) = 0 \qquad \text{on } B \tag{I}$$

or

$$\frac{\partial u}{\partial n}(x) = 0 \qquad \text{on } B \tag{II}$$

where $\frac{\partial}{\partial n}$ denotes the derivative along the normal, has an infinite number of non-negative eigenvalues with the associated eigenfunctions. We denote the eigenvalues and eigenfunctions by λ_n and $\omega_n(x)$ respectively[1] and assume that the eigenvalues are arranged according to non-decreasing order of magnitude and that the eigenfunctions form a complete normal orthogonal set. We observe, that in the case of the second boundary value problem viz. II, $\lambda_0 = 0$ is a simple eigenvalue with the eigenfunction $\omega_0(x) = \frac{1}{\sqrt{V}}$, where V is the volume of D, while in I, all the eigenvalues are positive. So it will be convenient to assume that the suffix n runs through $1, 2, 3, \ldots$ in case I and through $0, 1, 2, \ldots$ in case II and that $\lambda_1 > 0$.

With the above notations we have the following

THEOREM. *The series* $\sum_{n=1}^{\infty} \omega_n(x)\omega_n(y)/\lambda_n^s$, $s = \sigma + i\tau$, *which has a finite abscissa of absolute convergence, represents an entire function of* s, *if* x *and* y *are distinct points in* D, *with the so-called "trivial zeros" at* $s = 0, -1, -2, \ldots$ *in case* I *and at* $s = -1, -2, -3, \ldots$ *in case* II.

On the other hand the series $\sum_{n=1}^{\infty} \omega_n^2(x)/\lambda_n^s$ *which also has a finite abscissa of convergence, represents a meromorphic function of* s *with a simple pole at* $s = k/2$ *and residue* $1/\Gamma(k/2)(2\sqrt{\pi})^k$ *and with the so-called "trivial zeros" at* $s = 0, -1, -2, \ldots$ *in case* I *and at* $s = -1, -2, -3, \ldots$ *in case* II.

§ 3. The proof of the theorem depends on a lemma on the Green's function for the heat equation

$$\Delta u - \frac{\partial u}{\partial t} = 0 \tag{5}$$

which we state below. Let $G(x, y; t)$ denote the Green's function for the heat

[1] Each eigenvalue being repeated according to its multiplicity and the eigenfunctions being real.

equation (5) associated with either of the boundary conditions[2] I, II and further satisfying the initial condition

$$\lim_{t=0} G(x, y; t) = 0, \qquad x, y \text{ in } D,\ x \neq y.$$

It is known that $G(x, y; t)$ can be expressed in the form

$$G(x, y; t) = \frac{1}{(2\sqrt{\pi}t)^k} \exp\left(-\frac{\Sigma(x_i - y_i)^2}{4t}\right) - g(x, y; t) \tag{6}$$

where $\frac{1}{(2\sqrt{\pi}t)^k} \exp\left(-\frac{\Sigma(x_i - y_i)^2}{4t}\right)$ is the fundamental solution of (5). We have then the following

LEMMA. *If l_y denotes the minimum distance between y and points on B, then, in any finite interval of t,*

$$|g(x, y; t)| < \frac{c}{t^{k/2}} e^{-l_y^2/4t} \tag{7}$$

for all x in D, where c is a constant independent of x and t.

Assuming the lemma for the present we shall prove the theorem. We first observe that

$$G(x, y; t) = \sum \omega_n(x)\omega_n(y)e^{-\lambda_n t}$$

the summation on the right running from 1 to ∞ or 0 to ∞ according as the first or the second boundary condition is under consideration. So we can write the above equation in a more convenient form, viz.:

$$\sum_{n=1}^{\infty} \omega_n(x)\omega_n(y)e^{-\lambda_n t} = G(x, y; t) - \frac{\delta}{V} \tag{8}$$

where $\delta = 0$ or 1 according as I or II boundary problem is taken into consideration. Multiplying both sides of (8) by t^{s-1} and integrating with respect to t from 0 to ∞, we note that if $R(s)$ is sufficiently large the left side gives

$$\Gamma(s) \sum \omega_n(x)\omega_n(y)/\lambda_n^s \tag{9}$$

the series being absolutely convergent.[3] We now have to evaluate

$$\begin{aligned}
&\int_0^\infty \left(G(x, y; t) - \frac{\delta}{V}\right) t^{s-1}dt \\
&\quad = \int_0^1 \left(G(x, y; t) - \frac{\delta}{V}\right) t^{s-1}dt + \int_1^\infty \sum_{n=1}^{\infty} \omega_n(x)\omega_n(y)e^{-\lambda_n t}t^{s-1}dt \\
&\quad = \int_0^1 G(x, y; t)\, t^{s-1}dt - \frac{\delta}{s.V} + \int_1^\infty \sum_{n=1}^{\infty} \omega_n(x)\omega_n(y)e^{-\lambda_n t}t^{s-1}dt \qquad (10) \\
&\quad = -\frac{\delta}{sV} + \int_0^1 G(x, y; t)\, t^{s-1}dt + \sum \omega_n(x)\omega_n(y) \int_1^\infty e^{-\lambda_n t}t^{s-1}dt
\end{aligned}$$

if $R(s) > 0$.

[2] Though the Green's functions are different in the two boundary problems we use the same notation $G(x, y; t)$ and there need be no confusion.

[3] The iterated Green's function of Δu will belong to L_2 for a sufficiently high order of iteration, from which it will follow that $\Sigma\omega_n^2(x)/\lambda_n^\sigma$ is convergent if σ is large and $\Sigma\omega_n(x)\omega_n(y)/\lambda_n^\sigma$ will be absolutely convergent for large σ.

The last integral on the right of (10) is easily seen to be an entire function of s, while the second is

$$(11)\qquad \frac{1}{(2\sqrt{\pi})^k}\int_0^1 t^{s-k/2-1}\exp\left(-\frac{\sum_{i=1}^{k}(x_i-y_i)^2}{4t}\right)dt-\int_0^1 g(x,y;t)t^{s-1}dt.$$

The first integral in (11) is an entire function of s, if $x \neq y$ and the second is also an entire function of s on account of the lemma since $l_y \neq 0$ as long as y is an interior point. So combining (9) and (10) we note that

$$(12)\qquad \sum_{n=1}^{\infty}\frac{\omega_n(x)\omega_n(y)}{\lambda_n^s}+\frac{\delta}{V.\,\Gamma(s+1)}=\frac{E(s)}{\Gamma(s)}$$

where $E(s)$ denotes an entire function of s. (12) proves everything stated in the theorem about the series on the left. Incidentally it shows that while the analytic continuation of the Dirichlet's series vanishes at $s = 0$ in case I, it does not vanish in case II; in fact it takes the value $-\frac{1}{V}$.

If the two points x and y coincide, we have only to put $x = y$ in (9), (10), and (11) and observe that if $R(s)$ is large enough

$$\Gamma(s)\sum_{n=1}^{\infty}\omega_n^2(x)/\lambda_n^s=-\frac{\delta}{sV}+\frac{1}{(2\sqrt{\pi})^k}\cdot\frac{1}{s-k/2}$$

$$(13)\qquad -\int_0^1 g(x,x;t)\,t^{s-1}-\sum_{n=1}^{\infty}\omega_n^2(x)\int_1^{\infty}e^{-\lambda_n t}t^{s-1}dt.$$

While the last integral is easily seen to be an entire function of s, the last but one can be seen to be an entire function of s by the lemma as long as x is an interior point. Hence we have

$$(14)\qquad \sum_{n=1}^{\infty}\frac{\omega_n^2(x)}{\lambda_n^s}=\frac{1}{(2\sqrt{\pi})^k}\cdot\frac{1}{\Gamma(s)(s-k/2)}-\frac{\delta}{V\Gamma(s+1)}+\frac{E(s)}{\Gamma(s)}$$

which proves everything about $\Sigma\,\omega_n^2(x)/\lambda_n^s$ stated in the theorem.[4]

REMARKS: 1. It may be of interest to remark that by applying Ikehara's Tauberian theorem to (14) we obtain the following asymptotic distribution of eigenfunctions:

$$(15)\qquad \sum_{\lambda_n\leq T}\omega_n^2(x)\sim\frac{1}{(2\sqrt{\pi})^k\Gamma(k/2+1)}\,T^{k/2},$$

a result which can also be proved by applying Hardy-Littlewood's Tauberian theorem on Dirichlet's series to (8) with $x = y$ (see (2) in [5]).

[4] This series for the two dimensional domain was first studied by T. Carleman [1].

2. Another point of interest[5] is to study the nature of the series $\Sigma 1/\lambda_n^s$. If $R(s)$ is large and positive

$$\Gamma(s)\sum_{n=1}^{\infty} 1/\lambda_n^s = \int_D dx \int_0^1 \Sigma\omega_n^2(x)^{-\lambda_n t} t^{s-1}dt$$

$$= \int_D dx \int_0^1 + \int_D dx \int_1^\infty . \tag{16}$$

As usual the second integral on the right of (16) is an entire function while the first is

$$-\frac{\delta}{s} + \frac{V}{(2\sqrt{\pi})^k}\cdot\frac{1}{s-k/2} - \int_D dx \int_0^1 g(x,x;t)\, t^{s-1}dt$$

and by the lemma

$$\left|\int_D dx \int_0^1 g(x,x;t)\, t^{s-1}dt\right| \leq c\int_0^\infty dl_x \int_0^1 t^{\sigma-k/2-1}e^{-l_x^2/4t}dt$$

$$\leq c\int_0^\infty e^{-u}u^{-1}du \int_0^1 v^{\sigma-k/2-1}dv$$

on using the transformation $l_x^2/4t = u$; $t = v$. The above integral on the extreme right is finite if $\sigma > k/2 - \frac{1}{2}$, so that the first integral on the right of (16) is regular for $\sigma > k/2 - \frac{1}{2}$. Thus

$$\sum\frac{1}{\lambda_n^s} = -\frac{\delta}{\Gamma(s+1)} + \frac{V}{(2\sqrt{\pi})^k}\cdot\frac{1}{\Gamma(s)(s-k/2)} + \frac{F(s)}{\Gamma(s)} \tag{17}$$

where $F(s)$ is regular for $R(s) > k/2 - \frac{1}{2}$. Again by an application of Ikehara's Tauberian theorem to (17) we have the following well-known asymptotic distribution of eigenvalues: If $N(T)$ is the number of eigenvalues $\leq T$,

$$N(T) \sim \frac{V}{(2\sqrt{\pi})^k\Gamma(k/2+1)}\, T^{k/2}.$$

§ 4. Now it remains to prove the lemma. For this purpose we introduce slightly different notations. We denote by capital letters $P, Q \ldots$ points interior to D and by small letters $p, q, \ldots$ points on its boundary B. If $P = (x_1, \ldots, x_k)$, $Q = (y_1, \ldots, y_k)$ we write

$$r_{PQ}^2 = \sum_{i=1}^{k}(x_i - y_i)^2,$$

$$h_{\alpha\beta}(P, s; Q, t) = \frac{1}{(2\sqrt{\pi})^k}\,\frac{r_{PQ}^\alpha}{(t-s)^\beta}\exp\left(-\frac{r_{PQ}^2}{4(t-s)}\right),$$

$\cos r_{pq}n_p = \cos rn =$ cosine of the angle between the radius vector r_{pq} and the normal n_p at r. According to these notations

$$G(x, y; t) = G(P, Q; t) = h_{0,\,k/2}(P, 0; Q, t) - g(P, Q; t).$$

[5]The author is indebted to Professor H. Weyl for this remark.

As a function of (Q, t), $g(P, Q; t)$ is a solution of the heat equation tending to zero as $t \to 0$, and takes the same boundary values as $h_{0,\,k/2}$ on B for all t in case I, while in the case II its normal derivative has the same value as the normal derivative of $h_{0,\,k/2}$ on B.

We shall first prove the lemma in the case of the II boundary value problem. In this case we can set

$$g(P, Q; t) = \int_B \int_0^t h_{0,\,k/2}(p, s, Q, t)\psi(p, s)dpds \tag{18}$$

where $\psi(p, s)$ is an unknown function to be determined. It is clear our lemma will follow if we can show that a function $\psi(p, s)$ which is bounded in every finite interval $0 \leq s \leq T$, uniformly on B can be determined to satisfy (18). To show this we note that $\psi(p, s)$ is a solution of the following integral equation:

$$\psi(q, t) + \int_B \int_0^t h_{1,\,k/2+1}(p, s, q, t) \cos rn\psi(p, s)dpds$$

$$= \frac{\partial}{\partial n} g(p, q, t) = h_{1,\,k/2+1}(p, 0, q, t) = \phi(q, t), \tag{19}$$

say. Then $\psi(q, t)$ can be determined as a Neumann's series:

$$\begin{aligned} \psi(q, t) &= \phi_0(q, t) - \phi_1(q, t) + \phi_2(q, t) - \ldots, \\ \phi_0(q, t) &= \phi(q, t), \\ \phi_i(q, t) &= \int_B \int_0^t h_{1,\,k/2+1}(p, s; q, t) \cos rn\phi_{i-1}(p, s)dpds. \end{aligned} \tag{20}$$

If $|\phi(q, t)| \leq M$, as is certainly the case in $0 \leq t \leq T$, one proves by induction

$$|\phi_i(q, t)| \leq \frac{MN^i t^{i/2}}{\Gamma(i/2 + 1)}, \tag{21}$$

where N is a constant independent of t and i, which can be determined.[6] This shows that if $\phi(q, t)$ is bounded in any finite interval $0 \leq t \leq T$, so is $\psi(q, t)$. Hence the lemma.

Corresponding argument can be made use of in the case of the first boundary value problem.

References

[1] T. Carleman, "Propriétés asymptotiques des fonctions fondamentales des membranes vibrantes," *Scand. Math. Congress* (1934), 34-44.

[2] P. Epstein, "Zur Theorie allgemeiner Zetafunktionen I," *Math. Ann.*, vol. 56 (1903), 615-644.

[6] For a detailed discussion of these inequalities and the determination of the Green's function of the heat equation by Neumann's series cf. E. E. Levi [4, pp. 261-262.] We derive the inequality (21) assuming $\cos(rn) = 0(r)$ for small r. Similar inequalities can also be derived with $\cos(rn) = 0(r^a)$ $0 < a \leq 1$ which is a regularity condition on B.

[3] P. Epstein, "Zur Theorie allgemeiner Zetafunktionen II," *Math. Ann.*, vol. 63 (1907), 205-246.
[4] E. E. Levi, "Sull' equatione del calore," *Annali di Math.*, (3a), vol. 14 (1902), 187-264.
[5] S. Minakshisundaram, "Notes on Fourier Expansions II," *J. London Math. Soc.*, vol. 20 (1945), 148-153.

Andhra University

Supplementary Note by Hermann Weyl

At Minakshisundaram's request I add another proof of his fundamental lemma. This alternative proof is restricted to the boundary value problem I, but for this case yields a more complete result. Take for y a fixed interior point y_0 and set $l_{y_0} = l$. The maximum of the main part of Green's function along the boundary is

$$(4\pi t)^{-k/2} \exp(-l^2/4t) = j(t),$$

and this function $j(t)$ is on the increase as long as t moves from 0 to $T_0 = l^2/2k$.

Instead of splitting the integrals $\int_0^\infty$ into $\int_0^1 + \int_1^\infty$, as Minakshisundaram does, one splits into $\int_0^{T_0} + \int_{T_0}^\infty$. I maintain that in the first part, i.e. for $0 < t < T_0$, the compensating function $u(x; t) = g(x, y_0; t)$ satifies the inequality

$$0 \leq u(x; t) \leq j(t).$$

Proof. (1) For any t in this interval let $m(t)$ and $M(t)$ denote minimum and maximum of $u(x; t)$ as a function of x. Suppose that, contrary to the statement, $m(t_1)$ is negative for a certain t_1 between 0 and T_0, and that $u(x_1; t_1) = m(t_1)$. Since the boundary values of $u(x; t_1)$ are positive, x_1 must be an interior point, and one must have $\Delta u \geq 0$ for $x = x_1$, $t = t_1$. Hence the equation $\frac{\partial u}{\partial t} = \Delta u$ shows that $\frac{\partial u}{\partial t} \geq 0$ for the same values. Choose a positive constant a and form

$$v = e^{-at} \cdot u, \quad \frac{\partial u}{\partial t} - au = e^{at} \cdot \frac{\partial v}{\partial t};$$

one then sees that $\frac{\partial v}{\partial t} > 0$ for $x = x_1, t = t_1$. Hence $v(x_1; t)$ actually decreases during a short time, $t_1 \geq t \geq t'_1$, while t decreases starting with the value t_1. Set $e^{-at} \cdot m(t) = m^*(t)$. As $m^*(t) \leq v(x_1; t)$ we have *a fortiori* $m^*(t) \leq m^*(t_1)$ in that interval. Thus $m^*(t)$ goes down and continues to be negative while t decreases. That makes it possible to repeat the argument and to conclude that in the whole interval $t_1 \geq t > 0$ the function $m^*(t)$ decreases along with t

and thus stays less than or equal to $m^*(t_1)$. But this is a contradiction, since $v(x;t) \to 0$ for $t \to 0$.

(2) Suppose that, contrary to the proposition, $M(t_1) > j(t_1)$ for a definite value t_1 in the interval $0 < t_1 < T_0$. Then the maximum $M(t_1)$ is taken on at an interior point $x = x'_1$. We have $\Delta u \leq 0$ and hence $\frac{\partial u}{\partial t} \leq 0$ for $x = x'_1$, $t = t_1$, and thus $\frac{\partial u^*}{\partial t} < 0$ for the same values and $u^*(x;t) = u(x;t) - j(t)$. As $M(t) \geq u(x'_1;t)$, the "span" $M^*(t) = M(t) - j(t)$ thus increases during a short time while t decreases from t_1 downward. It therefore stays positive, and repetition of the argument shows that the span is increasing with decreasing t during the whole time $t_1 \geq t > 0$, a result that contradicts the limit equations $u(x;t) \to 0$, $j(t) \to 0$ for $t \to 0$.

Institute for Advanced Study

APPLICATIONS OF COMBINATORIAL FORMULAE TO GENERALIZATIONS OF WILSON'S THEOREM

N. S. MENDELSOHN

Summary. By the use of finite difference operators a series of combinatorial formulae are obtained. Two applications of the formulae are given. First, the following explicit formulae for the number, $f(n)$, of non-isomorphic equivalence relations among n elements are obtained:

$$f(n) = \sum_{k=1}^{n} \sum_{j=0}^{k} (-1)^j \frac{\binom{k}{j} (k-j)^n}{k!} = \sum_{k=1}^{n} \sum_{j=0}^{k} (-1)^j \frac{(k-j)^n}{j!(k-j)!};$$

$$f(n) = \frac{n^n}{n!}\left(\frac{1}{0!}\right) + \frac{(n-1)^n}{(n-1)!}\left(\frac{1}{0!} - \frac{1}{1!}\right) + \frac{(n-2)^n}{(n-2)!}\left(\frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!}\right) + \cdots$$

Second, by applying Fermat's theorem (i.e. $x^{p-1} \equiv 1 \bmod p$ for each prime p, which is prime to x) to the combinatorial formulae, we obtain a series of congruences which in a sense are generalizations of Wilson's theorem. The most general formula of this type is the following. Let n and k be arbitrary positive integers such that $k \geq n + 1$. There exists a positive integer $N(n, k)$ and a rational number $R(n, k)$, uniquely determined, such that

$$\int_0^1 \frac{dx_n}{x_n} \int_0^{x_n} \frac{dx_{n-1}}{x_{n-1}} \int_0^{x_{n-1}} \frac{dx_{n-2}}{x_{n-2}} \cdots \int_0^{x_3} \frac{dx_2}{x_2} \int_0^{x_2} \left\{\frac{(1-x_1)^{p-k} - 1}{x_1}\right\} dx_1$$

$$\equiv R(n, k) \bmod p$$

for all primes $p \geqslant N(n, k)$. The number $\max(n, 2k-2n-3)$ may be taken for $N(n, k)$. The proof of the theorem contains a method of computing $R(n, k)$. Such computations are not laborious for small n and k. As examples of such computations we quote the following formulae:

$$\int_0^1 \left\{\frac{(1-x)^{p-2} - 1}{x}\right\} dx \equiv -1 \bmod p, \text{ for all primes } p \geqslant 3;$$

$$\int_0^1 \frac{dt}{t} \int_0^t \left\{\frac{(1-x)^{p-3} - 1}{x}\right\} dx \equiv -\tfrac{1}{2} \bmod p, \text{ for all primes } p \geqslant 5.$$

Received September 1, 1948.

The author has also computed explicit formulae for some very general classes of cases of the main formulae. For example, if we denote

$$\int_0^1 \frac{dx_s}{x_s} \int_0^{x_s} \frac{dx_{s-1}}{x_{s-1}} \cdots \int_0^{x_3} \frac{dx_2}{x_2} \int_0^{x_2} \left\{ \frac{(1-x_1)^{p-t}-1}{x_1} \right\} dx_1$$

by $I_p\ (s, t)$ we have the following:

$$I_p\ (s, s+1) \equiv -\frac{1}{s!} \bmod p \text{ for all primes } p > s;$$

$$I_p\ (s, s+2) \equiv -\frac{(s+2)}{s!\ 2} \bmod p \text{ for all primes } p > s;$$

$$I_p\ (s, s+3) \equiv -\frac{(s+3)(3s+8)}{s!\ 24} \bmod p \text{ for all } p > \max\ (s, 3);$$

$$I_p\ (s, s+4) \equiv -\frac{(s+4)^2(s+3)}{s!\ 48} \bmod p \text{ for all } p > \max\ (s, 5).$$

The details of the computations are not given in the main body of the paper, but the method used differs in no way from that explained in the paper.

General Remarks. A number of papers have already appeared which deal with the use of finite difference operators for symbolic solutions of combinatorial problems. We content ourselves with three references [2], [3], and [4] in the bibliography. The operators we will use here are the standard operators E and Δ, defined as $Eu_n = u_{n+1}$ and $\Delta u_n = u_{n+1} - u_n$, with the obvious relation $E = 1 + \Delta$.

Consider a set of "triangular" equations connecting $u_0, u_1, \ldots, u_n$ with $v_0, v_1, \ldots, v_n$ by means of

$$\begin{aligned} v_0 &= c_{00}u_0 \\ v_1 &= c_{10}u_0 + c_{11}u_1 \\ v_2 &= c_{20}u_0 + c_{21}u_1 + c_{22}u_2 \\ &\cdot \\ &\cdot \\ &\cdot \\ v_n &= c_{n0}u_0 + c_{n1}u_1 + c_{n2}u_2 + \ldots + c_{nn}u_n. \end{aligned}$$

If $c_{00}c_{11}\ldots c_{nn} \neq 0$, the equations can be solved for $u_0, u_1, \ldots, u_n$ in terms of $v_0, v_1, \ldots, v_n$ in a unique way. Suppose the solved form of these equations is

$$\begin{aligned} u_0 &= d_{00}v_0 \\ u_1 &= d_{10}v_0 + d_{11}v_1 \\ &\cdot \\ &\cdot \\ &\cdot \\ u_n &= d_{n0}v_0 + d_{n1}v_1 + \ldots + d_{nn}v_n. \end{aligned}$$

It is immediately obvious how the d_{ij} may be obtained from the c_{ij} and conversely. However, we are interested in relating the d_{ij} to the c_{ij} by a symbolic equation. To this end we write both sets of equations as follows:

$$v_n = P_n(E)u_0, \text{ for } n = 0, 1, 2, 3, \ldots \tag{1}$$

$$u_n = Q_n(E)v_0, \text{ for } n = 0, 1, 2, 3, \ldots \tag{2}$$

where $P_n(E) = c_{n0} + c_{n1}E + c_{n2}E^2 + \ldots + c_{nn}E^n$ and $Q_n(E) = d_{n0} + d_{n1}E + d_{n2}E^2 + \ldots + d_{nn}E^n$. To obtain the symbolic equation connecting $d_{n0}, d_{n1}, \ldots, d_{nn}$ with c_{ij} we start with (2), $u_n = Q_n(E)v_0$; hence

$$E^n u_0 = d_{n0}v_0 + d_{n1}v_1 + d_{n2}v_2 + \ldots + d_{nn}v_n \tag{3}$$

and using (1) this becomes $E^n u_0 = \{d_{n0} + d_{n1}P_1(E) + d_{n2}P_2(E) + \ldots + d_{nn}P_n(E)\}u_0$. Hence $E^n = Q_n(P)$ symbolically, where it is understood that in computing the right-hand side P^i is to be replaced by $P_i(E)$. In the same way $E^n = P_n(Q)$ where Q^i is to be replaced by $Q_i(E)$. Hence, the relations connecting the d_{ij} with the c_{ij} are compactly expressed by the symbolic equation

$$P_n(Q) = E^n = Q_n(P). \tag{4}$$

The use of this general symbolic equation for the solution of combinatorial problems will be the subject of a subsequent paper. Here we will be concerned only with one particular case. Examples of pairs of polynomials $P_n(E)$ and $Q_n(E)$ which satisfy (4) are:

(a) $P_n(E) = \dfrac{1}{c_n}E^{n-1}\Delta$, and $P_0(E) = \dfrac{1}{c_0}$; $Q_n(E) = c_0 + c_1E + \ldots + c_nE^n$;

(b) $P_n(E) = (kE + r)^n$; $Q_n(E) = \dfrac{1}{k^n}(E - r)^n$;

(c) $P_n(E) = (1 + E)^n$; $Q_n(E) = \Delta^n$ (this is case (b) with $k = r = 1$);

(d) $P_n(E) = E^n - c_nE^{n-1}$; $Q_n(E) = E^n + c_nE^{n-1} + c_nc_{n-1}E^{n-2} + \ldots + c_nc_{n-1}c_{n-2}\ldots c_1$.

The equation to be used from here on is (c). More explicitly (c) is written as follows

$$\text{if}^1\ v_n = (E + 1)^n u_0$$

$$\text{then } u_n = \Delta^n v_0.$$

Applications. We consider first the following subsidiary problem. In how many ways can we place n distinguishable objects in m distinguishable boxes so that each box contains one object at least, the arrangement of the objects in the boxes being irrelevant. Let u_{mn} be the required number. The number of ways of placing the objects in the boxes without restriction is m^n. This can be broken up into the following exclusive cases: (1) no box is empty,

[1] This equation was pointed out to me by I. Kaplansky in 1938 and indirectly, in non-symbolic form, by Dean S. Beatty in 1935. It is implied by some of Poincaré's work. It first appeared explicitly (in non-symbolic form) in [1] which was published in 1938.

(2) one box is empty, (3) two boxes are empty, ..., $(m+1)$ all boxes are empty (vacuous). Hence,

$$(5) \qquad m^n = u_{mn} + \binom{m}{1} u_{m-1,n} + \binom{m}{2} u_{m-2,n} + \ldots + \binom{m}{m} u_{0n}.$$

Symbolically, this is written $m^n = (1+E)^m u_{0n}$. Hence, using (c) we obtain

$$(6) \qquad u_{mn} = \Delta^m 0^n = (E-1)^m 0^n.$$

Explicitly, this becomes

$$(7) \quad u_{mn} = m^n - \binom{m}{1}(m-1)^n + \binom{m}{2}(m-2)^n + \ldots + (-1)^{m-1}\binom{m}{m-1}.$$

We now apply (6) and (7) to the following problem.

How many non-isomorphic equivalence relationships do there exist among n objects? In combinatorial terms, this requires the determination of the number of ways of placing n distinct objects into any number of boxes, where we do not distinguish the boxes. If $f(n)$ be the required number, then obviously

$$f(n) = \sum_{i=1}^{n} \frac{u_{in}}{i!} + \sum_{i=1}^{n} \frac{\Delta^i 0^n}{i!}.$$

Hence we have

$$(8) \qquad f(n) = \sum_{k=1}^{n}\sum_{j=0}^{k} (-1)^j \binom{k}{j} \frac{(k-j)^n}{k!} = \sum_{k=1}^{n}\sum_{j=0}^{k} (-1)^j \frac{(k-j)^n}{j!(k-j)!}.$$

On inverting the order of summation, we obtain

$$(9) \quad f(n) = \frac{n^n}{n!}\left(\frac{1}{0!}\right) + \frac{(n-1)^n}{(n-1)!}\left(\frac{1}{0!} - \frac{1}{1!}\right) + \frac{(n-2)^n}{(n-2)!}\left(\frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!}\right) + \ldots$$

For a second application it is necessary to obtain alternative expressions for $u_{m,n}$. To this end we first note that $u_{mn} = 0$ if $n < m$. If $m = n$, then $u_{mn} = m!$ Applying this to (7) we obtain the well-known formula

$$(10) \quad m! = m^m - \binom{m}{1}(m-1)^m + \binom{m}{2}(m-2)^m + \ldots + (-1)^{m-1}\binom{m}{m-1}.$$

If $n = m+1$, to evaluate u_{mn} we note that the distribution of objects into boxes is such that two of the objects appear in one of the boxes, the remaining boxes each containing one object. The two objects to appear in one box may be chosen in $\binom{m+1}{2}$ ways, and hence the number of ways of distributing

the objects is $\binom{m+1}{2} m! = \frac{m}{2}(m+1)!$ Applying this to equation (7) we obtain

$$(11)\quad \frac{m}{2}(m+1)! = m^{m+1} - \binom{m}{1}(m-1)^{m+1} + \binom{m}{2}(m-2)^{m+1} + \ldots + (-1)^{m-1}\binom{m}{m-1}.$$

In case $n = m+2$ we can easily show that $u_{m,m+2}$ is given by

$$u_{m,m+2} = \binom{m+2}{3} m! + \frac{1}{2}\binom{m+2}{2}\binom{m}{2} m! = (m+2)!\left\{\frac{m(3m+1)}{24}\right\}.$$

(This comes from considering that the distribution is such that either two of the boxes each contain two objects, the remaining boxes containing one object, or one box contains three objects, the remaining boxes each containing one object.) Applying the above formula to equation (7) we obtain

$$(12)\quad \left\{\frac{m(3m+1)}{24}\right\}(m+2)! = m^{m+2} - \binom{m}{1}(m-1)^{m+2} + \binom{m}{2}(m-2)^{m+2} + \ldots + (-1)^{m-1}\binom{m}{m-1}.$$

In general, we wish to establish the following formula

$$(13)\quad (m+k)!\, P_k(m) = m^{m+k} - \binom{m}{1}(m-1)^{m+k} + \binom{m}{2}(m-2)^{m+k} + \ldots + (-1)^{m-1}\binom{m}{m-1}$$

where $P_k(m)$ is a polynomial in m of degree k with rational coefficients, for each integer k. We already have shown that

$$P_0(m) = 1,\ P_1(m) = \frac{1}{2}m \text{ and } P_2(m) = \frac{m(3m+1)}{24}.$$

Formula (13) is equivalent to the statement that

$$u_{m,m+k} = (m+k)!\, P_k(m).$$

To establish this statement we first note that $u_{m,n}$ satisfies the following recurrence:

$$(14)\quad u_{mn} = m u_{m,n-1} + m u_{m-1,n-1}.$$

Equation (14) for $n \geq m+2$ follows from the fact that the distribution of the

objects into the boxes may be carried out as follows: One of the objects may be placed in any one of the boxes (there are m ways of doing this) and the remaining $(n-1)$ objects may be distributed either amongst all the m boxes so that each box gets at least one object (there are $u_{m,n-1}$ ways of doing this) or they may be distributed amongst the $(m-1)$ boxes not occupied by the first object in such a way that each of these $(m-1)$ boxes gets at least one object (there are $u_{m-1,n-1}$ ways of doing this). Hence equation (14) follows.

If in (14) we replace n by $m+k$ and then put $u_{m,m+k}=(m+k)!\,P_k(m)$, we obtain

$$(m+k)P_k(m)=m\left\{P_{k-1}(m)+P_k(m-1)\right\}. \tag{15}$$

Equation (15) with the initial conditions $P_1(m)=\frac{m}{2}$, $P_k(1)=\frac{1}{(k+1)!}$ is sufficient to determine $P_k(m)$ for all positive integers k, and for all positive integers m. We proceed to show that $P_k(m)$ is a polynomial in m of degree k with rational coefficients. We will also show that the denominators of these coefficients (when expressed in their lowest terms) contain no prime factors greater than $2k-1$ except for $k=1$. The proof is by induction on k.

Since $P_1(m)=\frac{m}{2}$, $P_2(m)=\frac{m(3m+1)}{24}$ the theorem is true for $k=1$, $k=2$. Assume that $P_{k-1}(m)=c_{0,k-1}+c_{1,k-1}m+\ldots+c_{k-1,k-1}m^{k-1}$ where each of the $c_{i,k-1}(i=0,1,2,\ldots,k-1)$ is a rational number which when expressed in its lowest terms has a denominator no prime factor of which exceeds $2k-3$. Now put $P_k(m)=c_{0k}+c_{1k}m+c_{2k}m^2+\ldots+c_{kk}m^k$ (assuming that such a form exists). Substituting into (15) we obtain the equation

$$(m+k)\sum_{i=0}^{k}c_{ik}m^i=m\left[\sum_{i=0}^{k-1}c_{i,k-1}m^i+\sum_{i=0}^{k}c_{ik}(m-1)^i\right].$$

In this equation the terms in m^{k+1} on both sides of the equation have identical coefficients. On equating coefficients of m^k we obtain $2kc_{kk}=c_{k-1,k-1}$. This together with $c_{11}=\frac{1}{2}$ yields $c_{kk}=\frac{1}{2^k k!}$. Now let us assume that $c_{k-r,k}$ has been obtained for $r=0,1,2,\ldots s$. Taking the coefficient of m^{k-s-1} on each side we obtain

$$c_{k-s-2,k}+kc_{k-s-1,k}=c_{k-s-2,k-1}+\left\{c_{k-s-2,k}-\binom{k-s-1}{1}c_{k-s-1,k}+\binom{k-s}{2}c_{k-s,k}+\ldots+(-1)^{k-s-2}\binom{k}{k-s-2}c_{kk}\right\}.$$

Hence we obtain

$$(2k-s-1)c_{k-s-1,k}=c_{k-s-2,k-1}+\left\{\binom{k-s}{2}c_{k-s,k}-\binom{k-s+1}{3}c_{k-s+1,k}+\ldots+(-1)^{k-s-2}\binom{k}{k-s-2}c_{kk}\right\}.$$

Since all the terms on the right have already been computed this yields $c_{k-s-1,k}$. It is obvious that the denominator of $c_{k-s-1,k}$ has no prime factor greater than $2k-1$. This equation fails to yield the last coefficient c_{0k} but it is easily seen that $c_{0k}=0$ for $k=1, 2, 3, \ldots$. If we now put $m=1$ in (15) and use the fact that $P_k(0)=0$ (since $c_{0k}=0$) we obtain $(1+k)P_k(1)=P_{k-1}(1)$. From this it follows, since $P_1(1)=\frac{1}{2}$, that $P_k(1)=\frac{1}{(k+1)!}$. Hence, the initial conditions are satisfied. It is now obvious that if the polynomials $P_k(m)$ which have been determined by the above computation are substituted in equation (15), the equation is identically satisfied. Finally, since our initial conditions uniquely determine $P_k(m)$, the solution just found is the only possible one.

By specializing m in equation (13) and applying Fermat's theorem ($a^{p-1}\equiv 1 \bmod p$, if $(a, p)=1$ and p is prime) we can get the most general formula we are looking for. However, it will be instructive to start with the more particular formulae (10), (11), (12) to obtain completely explicit solutions for the first few cases.

If in (10) we put $m=p-1$ where p is a prime we obtain

$$(p-1)!=(p-1)^{p-1}-\binom{p-1}{1}(p-2)^{p-1}+\ldots+(-1)^{p-2}\binom{p-1}{p-2}.$$

Taking congruences mod p and applying Fermat's theorem we obtain

$$\begin{aligned}(p-1)!&\equiv 1-\binom{p-1}{1}+\binom{p-1}{2}+\ldots+(-1)^{p-2}\binom{p-1}{p-2}\\&\equiv(1-1)^{p-1}-1\equiv -1 \bmod p.\end{aligned}$$

This is, of course, Wilson's theorem, and the method of using formula (10) is well known, but the standard methods of obtaining formula (10) are different from the method employed here and do not generalize to formula (13). We prefer to write Wilson's theorem as follows:

$$(16)\qquad (p-r-1)!\equiv\frac{(-1)^{r+1}}{r!} \bmod p,\ (r=0, 1, 2, \ldots p-2).$$

If now in (10) we put $m=p-2$ where p is an odd prime we obtain

$$(p-2)!=(p-2)^{p-2}-\binom{p-2}{1}(p-3)^{p-2}+\binom{p-2}{2}(p-4)^{p-2}+\ldots+\binom{p-2}{p-3}.$$

Again applying Fermat's theorem to the right side of this equation and formula (16) to the left we obtain

$$1\equiv\frac{1}{p-2}-\binom{p-1}{1}\frac{1}{p-3}+\binom{p-2}{2}\frac{1}{p-4}+\ldots+\binom{p-2}{p-3} \bmod p.$$

The right-hand side of this congruence is precisely

$$-\int_0^1 \left\{\frac{(1-x)^{p-2}-1}{x}\right\} dx. \quad \text{Hence, } \int_0^1 \left\{\frac{(1-x)^{p-2}-1}{x}\right\} dx \equiv -1 \bmod p$$

for all odd primes p. In the same way if we replace m by $p-3$ in (10) we obtain

$$\int_0^1 \frac{dt}{t} \int_0^t \left\{\frac{(1-x)^{p-3}-1}{x}\right\} dx \equiv -\frac{1}{2} \bmod p \text{ for all primes } p \geq 5.$$

A few other particular cases have been worked out. For example, formula (11) with $m = p-3$ yields

$$\int_0^1 \left\{\frac{(1-x)^{p-3}-1}{x}\right\} dx \equiv -\frac{3}{2} \bmod p \text{ for all primes } p \geq 3.$$

Again formula (12) with $m = p-4$ yields $\int_0^1 \left\{\frac{(1-x)^{p-4}-1}{x}\right\} dx \equiv -\frac{11}{6}$ mod p for all primes $p \geq 5$. If in (13) we put $m = p-k-2$ and then $k = r-2$ we obtain in the same way the more general formula

$$(17) \qquad (-1)^{p-r} P_{r-2}(-r) \equiv \int_0^1 \left\{\frac{(1-x)^{p-r}-1}{x}\right\} dx \bmod p.$$

The left side of this formula is a rational number, which when expressed in its lowest terms, has a denominator with no prime factor greater than $2r-5$. Hence formula (17) is valid at least for all primes p which are greater than $2r-5$. (The case $k=1$, corresponding to $r=3$, is an exception.)

We now come to the most general case. In (13) put $m = p-k-r$, obtaining

$$(18) \quad (p-r)!\, P_k(p-k-r) = (p-k-r)^{p-r} - \binom{p-k-r}{1}(p-k-r-1)^{p-r} + \ldots + (-1)^{p-k-r-1}\binom{p-k-r}{p-k-r-1}.$$

Taking congruences mod p and using (16) and Fermat's theorem we obtain

$$(19) \quad \frac{(-1)^r}{(r-1)!} P_k(-k-r) \equiv \frac{1}{(p-k-r)^{r-1}} - \binom{p-k-r}{1}\frac{1}{(p-k-r-1)^{r-1}} + \ldots + (-1)^{p-k-r-1}\binom{p-k-r}{p-k-r-1}.$$

The right side of this congruence is equal to

$$(-1)^{p-k-r} \int_0^1 \frac{dx_{r-1}}{x_{r-1}} \cdots \int_0^{x_2} \frac{dx_2}{x_2} \int_0^{x_1} \left\{\frac{(1-x_1)^{p-k-r}-1}{x_1}\right\} dx_1.$$

Hence,

$$\frac{(-1)^r}{(r-1)!}P_k(-k-r)$$

$$\equiv (-1)^{p-k-r}\int_0^1 \frac{dx_{r-1}}{x_{r-1}}\cdots\int_0^{x_3}\frac{dx_2}{x_2}\int_0^{x_2}\left\{\frac{(1-x_1)^{p-k-r}-1}{x_1}\right\}dx_1 \bmod p.$$

If we put $r-1=s$ and $(k+r)=t$ in this equation we obtain

$$\frac{(-1)^{s-t}}{s!}P_{t-s-1}(-t)$$

$$\equiv \int_0^1 \frac{dx_s}{x_s}\cdots\int_0^{x_3}\frac{dx_2}{x_2}\int_0^{x_2}\left\{\frac{(1-x_1)^{p-t}-1}{x_1}\right\}dx_1 \bmod p. \tag{20}$$

If we write this in the form

$$\int_0^1 \frac{dx_s}{x_s}\cdots\int_0^{x_3}\frac{dx_2}{x_2}\int_0^{x_2}\left\{\frac{(1-x_1)^{p-t}-1}{x_1}\right\}dx_1 \equiv R(s,t) \bmod p \tag{21}$$

we have

$$R(s,t)=\frac{(-1)^{s-t}}{s!}P_{t-s-1}(-t).$$

This equation is valid for every odd prime p greater than the maximum of s and $2t-2s-3$. This condition is put on to ensure that $R(s,t)$ will not have denominators divisible by p. It is also necessary to have $t \geq s+1$ for our expression for $R(s,t)$ to be meaningful.

Our final result may be stated as follows. Let s and t be two positive integers such that $t \geq s+1$. There exists a rational number $R(s,t)$ such that (21) is valid for all primes $p \geq \max(s, 2t-2s-3)$. Also the number $R(s,t)$ is uniquely determined, since, if $T(s,t)$ were another number for which equation (21) is valid for all primes $p \geq$ some number p_0, then $R(s,t) \equiv T(s,t) \bmod p$ for all primes $p \geq$ some integer p_1. Putting $R(s,t)=\frac{a}{b}$ and $T(s,t)=\frac{c}{d}$, we have $ad \equiv bc \bmod p$, for all primes $p \geq \max(p_1, bd)$. Hence $ad=bc$ or $R(s,t)=T(s,t)$.

References

[1] H. Geirenger, *Ann. Math. Statist.*, vol. 9 (1938), 262.

[2] I. Kaplansky, "On a Generalization of the 'Problème des Rencontres'," *Amer. Math. Monthly*, vol. 46 (1939), 159-161.

[3] I. Kaplansky, "Symbolic Solution of Certain Problems in Permutations," *Bull. Amer. Math. Soc.*, vol. 50 (1944), 906-914.

[4] N. S. Mendelsohn, "Symbolic Solution of Card Matching Problems," *Bull. Amer. Math. Soc.*, vol. 52 (1946), 918-924.

University of Manitoba

AXIOMATIC TREATMENT OF RANK IN INFINITE SETS

R. RADO

1. Summary. In many branches of mathematics the notion of rank plays an important part. H. Whitney [3] made a detailed axiomatic investigation of rank and several related ideas. All sets considered by Whitney are finite. In the present note the axiomatic treatment of rank is extended to sets of any cardinal. In the special case of algebraic dependence of elements of a field with respect to a sub-field, similar questions have already been considered by Steinitz [2].

Following Whitney, we investigate rank by means of a function $r(A)$ which associates a non-negative integer with every finite subset A of a given set M and which satisfies axioms (4)-(6) below. These axioms state that (i) the empty set is of rank zero, (ii) by adding one more element to A the rank is either unaltered or increased by 1, (iii) if neither the addition of the element x nor the addition of the element y increases the rank of A then the simultaneous addition of both, x and y, does not increase the rank of A. A subset L of M is called *independent*, if the rank $r(A)$ of every finite subset A of L is equal to the number of elements of A. A *base* of L is a maximal independent subset of L, i.e. an independent subset of L which is not a proper subset of another independent subset of L. It is easy to prove that every subset L of M possesses at least one base, more generally, that every independent subset of L is contained in some base of L. The main result of this note is that all bases of L have the same cardinal. Thus it is possible to define the rank $r(L)$ of any subset L of M as the common cardinal of all bases of L or, which is equivalent, as the largest cardinal of independent subsets of L.

Lemma 1 is a general combinatorial theorem which is capable of various applications. Lemma 2 generalizes an earlier theorem[1] on axiomatically defined independence of elements of a set.

2. A combinatorial lemma. We require a lemma which, in a certain sense, can be considered as a generalization of Cantor's diagonal process. Let there be given a system of finite, non-empty sets A_ν, where the index ν ranges over an arbitrary set, the index set. Corresponding to every finite set $N = \{\nu_1, \nu_2, \ldots, \nu_m\}$ of indices, select arbitrarily one element from each of the sets $A_{\nu_1}, A_{\nu_2}, \ldots, A_{\nu_m}$. This means that the element selected, say, from A_{ν_1}, depends not only on ν_1 but also on the particular index set N of which ν_1 is a member. The assertion is that, under these circumstances, it is possible to make one

Received September 1, 1948.

[1] [1], Theorem 3.

further selection of elements, this time of one element x^*_ν from each A_ν, so that the following condition holds. However one chooses a finite index set N, there exists a finite index set N' containing N, such that, for every index ν of N, the element selected from A_ν in the given selection corresponding to the index set N', is x^*_ν.

Let M be an arbitrary set. Typical elements of M are denoted by the letters x and y, and typical finite subsets of M are denoted by A and B. Let M_1 be another set. Letters ν and N denote typical elements and finite subsets of M_1 respectively.

LEMMA 1. *Let* $A_\nu \subset M (\nu \epsilon M_1)$. *Suppose that the elements* $x(N, \nu)$ *satisfy*

$$x(N, \nu) \epsilon A_\nu \quad (\nu \epsilon N \subset M_1).$$

Then there are elements x^*_ν *such that, given any* N, *there exists* N' *satisfying* $N \subset N'$,

$$x^*_\nu = x(N', \nu) \quad (\nu \epsilon N).$$

Proof. We say that a system of sets $B_\nu (\nu \epsilon M_1)$ has the property R (possesses representatives) if, given any N, there exists N' satisfying $N \subset N'$,

$$x(N', \nu) \epsilon B_\nu \quad (\nu \epsilon N).$$

By hypothesis, the system A_ν possesses the property R, in fact, with $N' = N$. The assertion of the lemma is that there are elements x^*_ν such that the system $\{x^*_\nu\}$ has the property R.

We may assume that[2] $MM_1 = \theta$. Let M and M_1 be well-ordered.[3] The order relation is denoted by "$<$". Let $\bar{\nu}$ be the first element of M_1. Since $x(\{\nu\}, \nu) \epsilon A_\nu$, we have $A_\nu \neq \theta$. We shall define elements x_ν inductively. Let $\nu_0 \epsilon M_1$, and suppose that x_ν has already been defined for all $\nu < \nu_0$, and that $x_\nu \epsilon A_\nu (\nu < \nu_0)$. This includes the case $\nu_0 = \bar{\nu}$, when no assumption is made about the existence of elements x_ν. Consider the following systems of sets:

$$\text{system } S(\nu_0): \qquad B_\nu(\nu_0) = \begin{cases} \{x_\nu\} & (\nu < \nu_0) \\ A_\nu & (\nu \geqq \nu_0) \end{cases}$$

$$\text{system } S'(\nu_0, x): \qquad B'_\nu(\nu_0, x) = \begin{cases} \{x_\nu\} & (\nu < \nu_0) \\ \{x\} & (\nu = \nu_0) \\ A_\nu & (\nu > \nu_0). \end{cases}$$

Case 1. Suppose that $S(\nu_0)$ does not possess the property R. Then define x_{ν_0} to be the first element of A_{ν_0}.

Case 2. Suppose that $S(\nu_0)$ possesses the property R. Then x_{ν_0} is defined as the first element x of A_{ν_0} which satisfies the condition that $S'(\nu_0, x)$ possesses the property R. It must now be shown that there exists such an element x. Let us therefore assume that for no x of A_{ν_0} the system $S'(\nu_0, x)$ has the prop-

---

[2] $\{X, Y, \dots\}$ denotes the set whose elements are $X, Y, \dots$. $S + T$ and ST are the union and meet of sets S and T respectively, and $S - ST$ is the set of elements of S not belonging to T. The empty set is denoted by θ, and the cardinal of S is $|S|$.

[3] The well-ordering of M can be dispensed with.

erty R. Then, given any $x \epsilon A_{\nu_0}$, there is $N(x)$ satisfying the following condition. For no N' containing $N(x)$ is

(1) $$x(N', \nu) \epsilon B'_\nu(\nu_0, x) \qquad (\nu \epsilon N(x)).$$

Put $$N^* = \sum_{x \epsilon A_{\nu_0}} N(x).$$

Then N^* is finite. Since $S(\nu_0)$ has the property R, there exists N' satisfying $N^* \subset N'$,

(2) $$x(N', \nu) \epsilon B_\nu(\nu_0) \qquad (\nu \epsilon N^*).$$

Let $x \epsilon A_{\nu_0}$. Then $N(x) \subset N^* \subset N'$. Hence, by the assumption which we want to prove false, (1) does not hold. By (2),

(3) $$x(N', \nu) \epsilon B_\nu(\nu_0) \qquad (\nu \epsilon N(x)).$$

By comparing (1) and (3), one concludes that, for some $\nu \epsilon N(x)$,

$$B'_\nu(\nu_0, x) \neq B_\nu(\nu_0).$$

Therefore $$\nu_0 \epsilon N(x) \subset N^* \ (x \epsilon A_{\nu_0}).$$

Put $x(N', \nu_0) = x'$. Then

$$x' \epsilon A_{\nu_0};\ x(N', \nu) \epsilon B'_\nu(\nu_0, x') \quad (\nu \epsilon N(x')),$$

in contradiction to the assumption that (1) is false for every x of A_{ν_0}. Hence this assumption is false, and it is possible to define an element x_{ν_0} in the way indicated. Thus, by transfinite construction, one obtains elements $x_\nu \epsilon A_\nu$ which satisfy the following condition C: if, for some ν_0, the system $S(\nu_0)$ has the property R, then the system $S'(\nu_0, x_{\nu_0})$ has the property R.

Put $$S'(\nu_0, x_{\nu_0}) = S^*(\nu_0),$$

$$B'_\nu(\nu_0, x_{\nu_0}) = B^*_\nu(\nu_0).$$

By the hypothesis of the lemma, $S(\bar{\nu})$ has the property R. Hence, by condition C, $S^*(\bar{\nu})$ has the property R. Let $\nu_0 > \bar{\nu}$, and assume that, for every $\nu_1 < \nu_0$, $S^*(\nu_1)$ has the property R. Consider any set N. Since N is finite, there is an element $\nu_1 < \nu_0$ satisfying

$$\nu \leq \nu_1 \quad (\nu \epsilon N;\ \nu < \nu_0).$$

Since $S^*(\nu_1)$ has the property R, there exists N' satisfying

$$N \subset N';\ x(N', \nu) \epsilon B^*_\nu(\nu_1) \qquad (\nu \epsilon N).$$

Then $$x(N', \nu) \epsilon B^*_\nu(\nu_1) \subset B_\nu(\nu_0) \qquad (\nu \epsilon N).$$

Since N is arbitrary, this shows that $S(\nu_0)$ has the property R. Hence, by condition C, $S^*(\nu_0)$ has the property R. Thus it follows by induction that every system $S^*(\nu)$ has the property R.

Let $N \neq \theta$. Let ν' be the last element of N. Since $S^*(\nu')$ has the property R, there exists N' such that

$$N \subset N';\ x(N', \nu) \epsilon B^*_\nu(\nu') = \{x_\nu\} \quad (\nu \epsilon N),$$

$$x_\nu = x(N', \nu) \quad (\nu \epsilon N).$$

Hence the assertion of the lemma is true for $x^*_\nu = x_\nu$.

I should like to point out that the lemma is no longer valid if in both, hypothesis and conclusion, the condition that A and N are finite sets, is replaced by the condition that A and N are at most denumerable sets. For let M be the set of all positive integers and M_1 be a non-denumerable set, $A_\nu = M$ $(\nu \in M_1)$. If N is at most denumerable, say[4] $N = \{\nu_1, \nu_2, \dots\}_{\neq}$, define $x(N, \nu)$, for $\nu \in N$, by putting $x(N, \nu_\lambda) = \lambda$ $(\nu_\lambda \in N)$. Then the modified hypothesis holds, but the modified conclusion of the lemma does not hold.

3. A lemma on rank functions. We use the notation of sec. 2. In addition, we denote by L any subset of M. By definition, a *rank function* in M is a function r which associates with every A an integer $r(A)$ and satisfies the following axioms[5]:

$$r(\theta) = 0, \tag{4}$$

$$r(A) \leq r(A + \{x\}) \leq r(A) + 1, \tag{5}$$

$$\begin{cases} \text{if} & r(A) = r(A + \{x\}) = r(A + \{y\}), \\ \text{then} & r(A) = r(A + \{x, y\}). \end{cases} \tag{6}$$

Put $f(L) = 1$, if $r(A) = |A|$ $(A \subset L)$, and $f(L) = 0$ otherwise. In particular, $f(\theta) = 1$. The equation $f(L) = 1$ expresses the fact that the set L is independent, in the sense of this term as defined in the summary of this note.

Let A_ν be a system of finite subsets of M which has the property that, given any finite number k of distinct indices ν_κ, the union of the corresponding k sets A_{ν_κ} is at least of rank k. Then Lemma 2 below states that it is possible to select one element from each A_ν in such a way that the selected elements are mutually distinct and the set of all selected elements is independent.

LEMMA 2. *Let $r(A)$ be a rank function in M. Let*

$$A_\nu \subset M \quad (\nu \in M_1).$$

Suppose that

$$r\Big(\sum_{\nu \in N} A_\nu\Big) \geq |N| \quad (N \subset M_1). \tag{7}$$

Then there are elements $x^*_\nu \in A_\nu$ satisfying

$$x^*_{\nu_1} \neq x^*_{\nu_2} \quad (\nu_1 \neq \nu_2), \tag{8}$$

$$f\Big(\sum_{\nu \in M_1} \{x^*_\nu\}\Big) = 1. \tag{9}$$

Clearly, (7) is necessary for the existence of such x^*_ν.

Proof. Whitney[6] has shown that the definition of a rank function r in M satisfying (4), (5) and (6) is equivalent to a classification of all finite subsets of M into dependent and independent sets, this classification satisfying certain axioms.[7] Given the definition of rank, Whitney's definition of independence is identical with the definition given in the present note. Actually in Whitney's

[4] The symbol $\{X, Y, \dots\}_{\neq}$ denotes the set $\{X, Y, \dots\}$ and, at the same time, expresses the fact that the objects $X, Y, \dots$ are different from each other.

[5] [3], 510, $(R_1)-(R_3)$.

[6] [3], 6.

[7] [3], 513, (I_1) and (I_2).

case, M is finite, but in this particular instance no use is made of this fact. In view of Whitney's result, the case of Lemma 2 in which M_1 is finite is contained in a known theorem.[8] Now let M_1 be of any cardinal. Then, by applying this last result to a finite subset N of M_1, one can find elements $x(N, \nu)$ satisfying

$$x(N, \nu) \in A, \ (\nu \in N \subset M_1),$$

$$r(\sum_{\nu \in N} \{x(N, \nu)\}) = |N| \quad (N \subset M_1). \tag{10}$$

By Lemma 1, there are elements x^*_ν satisfying

$$x^*_\nu = x(N', \nu) \quad (\nu \in N \subset M_1),$$

where $N' = N'(N)$ is a certain set containing N. Put

$$A = A(N) = \sum_{\nu \in N} \{x(N', \nu)\} \ ; \ B = B(N) = \sum_{\nu \in N' - N} \{x(N', \nu)\} .$$

Then, by using (10) and two simple results of (1),[9] one deduces that

$$|N'| = r(A + B) \leq r(A) + r(B) \leq |A| + |B| \leq |N| + |N' - N| = |N'| ,$$

$$r(A) = |A| = |N| ,$$

$$r(\sum_{\nu \in N} \{x^*_\nu\}) = r(\sum_{\nu \in N} \{x(N', \nu)\}) = r(A) = |N| .$$

This implies (8) and (9).

4. The rank of sets of any cardinal. We use the same notation as in the preceding section. Let $r(A)$ be a rank function defined in M. Let L be a subset of M. A subset L^* of L is called a base of L, if L^* is a maximal independent subset of L, i.e. if

$$f(L^*) = 1 \ ; \ f(L^* + \{x\}) = 0. \qquad (x \in L - L^*).$$

I shall now prove that the concepts of independence and base relating to sets of any arbitrary cardinal have some of the usual properties well known in the case of finite sets, in particular that (i) given two independent sets, the second of higher cardinal than the first, it is possible to enlarge the first by the addition of one more element of the second set in such a way that independence is not lost; (ii) every independent subset of a set is contained in some base of this set; (iii) all bases of a set are of the same cardinal.

THEOREM. (i) *If* $|L| < |L'|$; $f(L) = f(L') = 1$, *then there exists* $x' \in L' - LL'$ *satisfying* $f(L + \{x'\}) = 1$.

(ii) *If* $L_1 \subset L$; $f(L_1) = 1$, *then there exists a base of* L *which contains* L_1. *In particular* (L_1 *the empty set*) *every set* L *possesses at least one base.*

(iii) *If* L' *and* L'' *are bases of* L, *then* $|L'| = |L''|$.

In view of (ii) and (iii), one can define the *rank cardinal* $r(L)$ as the largest cardinal of independent subsets of L, or, which is equivalent, as the common cardinal of all bases of L. If L is finite, this definition is consistent with the given definition of r.

---

[8] [1], Theorem 3.

[9] [3], (3.3) and Lemma 1.

Proof. For every integer $n \geqq 0$ and every ordered system $x_1, x_2, \ldots, x_n$ of n elements of M, define a number $I(x_1, \ldots, x_n)$ as follows:

$$I(x_1, \ldots, x_n) = 1, \text{ if } r(\{x_1, \ldots, x_n\}) = n,$$
$$I(x_1, \ldots, x_n) = 0 \text{ otherwise.}$$

According to Whitney,[10] the function I satisfies conditions (i)-(iv) of [1], in particular

$$I(y_1, \ldots, y_m)\, I(x'_1, \ldots, x'_{m+1}) \leq \sum_{\mu=1}^{m+1} I(y_1, \ldots, y_m, x'_\mu). \tag{11}$$

In order to prove (i) of the Theorem, assume that

$$f(L + \{x\}) = 0, \quad (x \in L' - LL'). \tag{12}$$

Let $x' \in L'$. Then there exists a set $\{x_1, \ldots, x_n\}_{\neq} \subset L$ satisfying

$$I(x_1, \ldots, x_n, x') = 0. \tag{13}$$

For if $x' \in L$, this follows from (12). If $x' \in L$, (13) holds for $n = 1$, $x_1 = x'$. Put, for some fixed choice of n and $x_1, \ldots, x_n$, $\{x_1, \ldots, x_n\} = A(x')$. I want to apply Lemma 2 to the system of sets $A(x')$ $(x' \in L')$, using the cardinal number as the rank function occurring in Lemma 2. In order to verify (7) assume that

$$\{x'_1, \ldots, x'_k\}_{\neq} \subset L',$$
$$A(x'_1) + \ldots + A(x'_k) = \{y_1, \ldots, y_m\}_{\neq} \subset L, \tag{14}$$
$$m < k.$$

This should lead to a contradiction. By (13),

$$I(y_{m_1}, \ldots, y_{m_l}, x'_1) = 0$$

for suitable m_λ; $1 \leq m_1 < \ldots < m_l \leq m$. Then $I(y_1, \ldots, y_m, x'_1) = 0$ and, by symmetry,

$$I(y_1, \ldots, y_m, x'_\kappa) = 0 \qquad (1 \leqslant \kappa \leqslant k). \tag{15}$$

Since $f(L) = 1$,

$$I(y_1, \ldots, y_m) = 1. \tag{16}$$

One deduces from (14), (16), (15), (11) that $I(x_1', \ldots, x'_k) = 0$, which contradicts $f(L') = 1$. This proves that

$$|A(x'_1) + \ldots + A(x'_k)| \geqslant k$$

whenever $\{x'_1, \ldots, x'_k\}_{\neq} \subset L'$. Hence, by Lemma 2, one can find elements $\phi(x')$ satisfying

$$\phi(x') \in A(x') \subset L \qquad (x' \in L'),$$
$$\phi(x') \neq \phi(x'') \text{ for } x' \neq x''.$$

This contradicts the fact that $|L'| > |L|$. Hence (i) holds.

In order to prove (ii), suppose that $L_1 \subset L$; $f(L_1) = 1$. Let Λ be the aggregate whose elements are all sets L' satisfying $L_1 \subset L' \subset L$; $f(L') = 1$. Thus $L_1 \in \Lambda$. Then Zorn's Lemma [4] applies to Λ. For let Λ' be any subaggregate of Λ which has the property that, whenever $L' \in \Lambda'$, $L'' \in \Lambda'$, at least one of the

[10] [3], 6.

relations $L' \subset L''$, $L'' \subset L'$ holds; denote by L''' the union of all sets $L' \in \Lambda'$. Then, clearly, any finite subset A of L''' is subset of some element of Λ', and hence satisfies $f(A) = 1$. Therefore $f(L''') = 1$, $L''' \in \Lambda'$. By Zorn's Lemma, Λ possesses a maximal element L^*. This means that

$$L_1 \subset L^* \subset L;\ f(L^*) = 1,$$
$$f(L^* + \{x\}) = 0 \qquad (x \in L - L^*),$$

i.e. that L^* is a base of L containing L_1. This proves (ii).

Finally, suppose that L' and L'' are bases of L, $|L'| < |L''|$. Then $f(L') = f(L'') = 1$. Hence, by (i), there exists $x' \in L'' - L'L''$ such that $f(L' + \{x'\}) = 1$. This contradicts the fact that L' is a base of L and hence, by definition, not a proper subset of an independent subset of L. This completes the proof of the theorem.

References

[1] R. Rado, "A Theorem on Independence Relations," *Quart. J. Math.*, vol. 13 (1942), 83-89.

[2] E. Steinitz, "Algebraische Theorie der Körper," *Crelle* 137 (1909).

[3] H. Whitney, "On the Abstract Properties of Linear Dependence," *Amer. J. Math.*, vol. 57 (1935), 509-533.

[4] Zorn, "A Remark on Method in Transfinite Algebra," *Bull. Amer. Math. Soc.*, vol. 41 (1935), 667.

King's College, London

REPRESENTATION BY QUADRATIC FORMS

GORDON PALL

1. Introduction. The elementary portions of the theory of integral representation of numbers or forms by quadratic forms will be somewhat simplified and generalized in this article. This indicates certain directions in which new applications can be made. The applications made here will be largely to the representation of numbers or binary quadratic forms by ternary quadratic forms. Particularly, we shall obtain the correct estimate (Theorem 10) needed to fill a lacuna in certain work of U. V. Linnik [1] on the representation of large numbers by ternary quadratic forms. Since Linnik applied his theorem on ternaries to prove [9] that every large number is a sum of at most seven positive cubes, a lacuna in this proof can now be regarded as filled.

While a genus, consisting of a finite number of classes of forms, is *regular* in the sense that one or other of its classes represents any number not trivially excluded by the generic conditions, it is difficult to prove anything general about the numbers representable separately by a single class. Thus, for example, $x^2+y^2+7z^2$ and $x^2+2y^2-2yz+4z^2$ are representative forms (one from each class) of the two classes of a certain genus, and represent between them all (and only) the positive integers not of the forms $7^{2k+1}(7n+r)$, $(r = 3, 5, 6)$. But a given number (e.g. 3) not of the excluded forms may happen to be represented by one class but not the other. In this example it can be proved that each class represents all positive integers congruent to 0 or 1 mod 4 and not of the excluded type $7^{2k+1}(7n+r)$, and there is some reason to believe that all "large" numbers represented by either form are represented by the other. Although general theorems stating that single classes are regular for large numbers have been proved (Kloosterman [2], Tartakowsky [3], Ross and Pall [4]) for forms in four and more variables, the situation is more complicated in the case of positive ternary quadratic forms.

Examples illustrating this were published by the author in 1939 [5]. Thus, the forms $f = x^2+y^2+16z^2$ and $g = 2x^2+2y^2+5z^2-2xz-2yz$ represent the two classes of a certain genus of determinant 16. It was proved that g represents no square m^2 such that all the prime factors of m are congruent to 1 mod 4. Since f obviously represents all squares, it is clear that g does not represent all the large numbers represented by its genus. The example shows also that, in general, a class may not represent the numbers consistent with its genus and divisible by a large square factor.

It may be of interest to state another property of f and g, that by combining classical results of Glaisher [6] with results on the representation of numbers

Received September 1, 1948.

$8n+1$ in the Jones-Pall article mentioned earlier, one obtains precise formulae for the number of representations $f(n)$ and $g(n)$ of an arbitrary integer n by f and g. This is believed to be the first known example among genera of forms in more than two variables. If $r_0(n)$ denotes the number of representations of n as a sum of three squares (for which there are well-known expressions), then

$$\begin{aligned}
f(n) &= g(n) = r_0(n)/3 \text{ if } n \equiv 2 \text{ or } 5 \bmod 8;\\
f(n) &= g(n) = 0 \qquad \text{if } n \equiv 3, 6, \text{ or } 7 \bmod 8;\\
f(n) &= g(n) = (1 - j/3)r_0(n) \text{ if } n = 4(4k + j),\ j = 0, 1, 2, 3;\\
f(n) &- g(n) = 0 \qquad \text{if } n \equiv 1 \bmod 8,\ n \text{ not square},\\
&= (-1)^{\frac{1}{2}(s-1)}4s \quad \text{if } n = s^2,\ s \text{ odd and positive};\\
f(n) &+ g(n) = 2r_0(n)/3 \text{ if } n \equiv 1 \bmod 8.
\end{aligned}$$

Linnik [1] obtained, by means of generalized quaternions, a theorem stating that under certain conditions (which are not satisfied by the preceding example) a class of positive-definite, ternary quadratic forms represents the sufficiently large odd numbers prime to the determinant which its genus represents. At a certain stage of his proof, he reduces the problem to that of representing a binary quadratic form $\phi = k\phi_1$(ϕ_1 properly or improperly primitive) as the sum of squares of three linear forms

$$(a_1x + b_1y)^2 + (a_2x + b_2y)^2 + (a_3x + b_3y)^2$$

such that the g.c.d. of the numbers $a_2b_3 - a_3b_2$, $a_3b_1 - a_1b_3$, $a_1b_2 - a_2b_1$ is equal to the divisor k of ϕ. Later, ϕ is thus represented by a more general ternary quadratic form. He states that if D denotes the determinant of ϕ then for every positive ϵ, the number of such representations of ϕ is of the order $0(D^{\epsilon})$; and that "this can be proved by methods similar to those of Gauss." Classical treatments (e.g. in [7]) seem, however, to have been restricted to the case where the divisor k of ϕ is squarefree; and Linnik's statement is in fact not true in general. The true estimate is given in Theorems 4 and 5, and involves the factor h, where h^2 is the largest square factor common to k and $ab - t^2$, where $\phi_1 = ax^2 + 2txy + by^2$; thus h can be as large as $D^{1/6}$.

Fortunately, the forms in which h is large can be counted differently, and hence Linnik's applications can be carried through successfully. This was indicated by the author [8] in 1941 for the special case of ordinary quaternions and a sum of three squares.

Notations. Unless otherwise indicated, capital letters $A, \ldots, Z$ denote matrices. The symbol $T_1^{(n,k)}$ indicates that T_1 has n rows and k columns. $A, \ldots, G$ are symmetric. German letters $\mathfrak{x}$, $\mathfrak{y}$, $\mathfrak{t}$ designate column vectors. T^{T} denotes the transpose of T. I is an identity matrix; a zero matrix is denoted by 0; p is a prime. The determinant of a quadratic form $f = \mathfrak{x}'A\mathfrak{x}$ is denoted by $|f|$ or $|A|$. The form $\phi_1 = ax^2 + 2txy + by^2$ is properly primitive (*p.p.*) if a, $2t$, and b are relatively prime (a, t, b integers); improperly primitive (*i.p.*) if a, t, b are relatively prime and a, b are even. The terms *unimodular* and *unit-modular* designate integral square matrices of respective determinants 1 and ± 1.

2. Integral and primitive representations. Let $A^{(n,n)}$ and $B_1^{(k,k)}$ be non-singular, symmetric, real matrices, $1 \leq k \leq n$. We say that A *represents* B_1 if there exists an integral matrix $T_1^{(n,k)}$ such that

$$T^{\mathsf{T}}_1 A T_1 = B_1; \tag{1}$$

and we call T_1 a *representation* of B_1 *by* A. Also, T_1, or $\mathfrak{x} = T_1\mathfrak{y}$, is called a representation of the quadratic form $\mathfrak{y}^{\mathsf{T}}B_1\mathfrak{y}$ by the quadratic form $\mathfrak{x}^{\mathsf{T}}A\mathfrak{x}$. Note that since a representation is a matrix, two representations are considered as equal only if corresponding components are equal. Thus the solution $x = 7$, $y = 4$ of $x^2 + y^2 = 65$ gives rise under permutations and sign-changes to eight representations of 65 by the form $x^2 + y^2$, or by its matrix I.

In a similar manner, since $T^{\mathsf{T}}_1(W^{\mathsf{T}}AW)T_1 = (WT_1)^{\mathsf{T}}A(WT_1)$, where W is any unimodular automorph of A, the matrix WT_1 is a representation of B_1 by A, with T_1. As W ranges over all the unimodular automorphs of A, the set of matrices WT_1 will be called a *set of representations*, and denoted by (WT_1).

If the g.c.d. μ of the minor determinants of order k in T_1 is 1, the representation is termed *primitive*. If A and B_1 are integral, the problem of finding the representations of B_1 by A can be reduced to that of finding the primitive representations of a certain finite set of matrices by A. We use for this purpose the following lemma.

LEMMA 1. *Let $T_1^{(n,k)}$ be an integral matrix of g.c.d. μ, $1 \leq k \leq n$. Then T_1 can be expressed in one and only one way in the form*

$$T_1 = R_1 M, \tag{2}$$

where $R_1^{(n,k)}$ is primitive, $M^{(k,k)}$ is integral, $|M| = \mu$, and M has the form

$$\begin{bmatrix} \mu_1 & \mu_{12}, \ldots, \mu_{1k} \\ 0 & \mu_2, \ldots, \mu_{2k} \\ \cdot & \cdot \quad \cdot \quad \cdot \quad \cdot \\ 0 & 0, \ldots, \mu_k \end{bmatrix}, \qquad \begin{matrix} \mu_1, \ldots, \mu_k = \mu, \\ 0 \leqq \mu_{ji} < \mu_i \ (i = 2, \ldots, k; j < i), \end{matrix} \tag{3}$$

where the elements $\mu_1, \ldots, \mu_k$ are positive integers, the elements μ_{ji} above each μ_i, are integers reduced modulo μ_i, and those below the principal diagonal are 0.

Proof. By Lemma 3 below, we can obtain (2) with R_1 primitive, and M merely integral and of determinant μ, but have the possibility of replacing R_1 by R_1V^{-1} and M by VM, with V unimodular. Hence the lemma is a consequence of the following result, first given for a general k by C. Hermite [11].

LEMMA 2. *If $M^{(k,k)}$ is integral, and $|M| = \mu > 0$, then by choice of a unimodular matrix V, VM can be made equal to one and only one Hermite-matrix* (3).

If we substitute $T_1 = R_1M$ in (1), we have

$$R^{\mathsf{T}}_1 A R_1 = B'_1, \text{ where } B'_1 = (M^{\mathsf{T}})^{-1}B_1M^{-1}, \tag{4}$$

and the left member is an integral, symmetric matrix. Hence

$$B_1 = M^{\mathsf{T}}B'_1M, \tag{5}$$

where B'_1 is integral. Thus μ^2 is restricted to be one of the finitely many square factors of $|B_1|$, and hence the Hermite-matrix M has only a finite number

of possible values. *All the representations of B_1 by A are found, without duplication, in the formula $T_1 = R_1 M$, where M ranges over the Hermite-matrices* (3) *such that $(M^T)^{-1} B_1 M^{-1}$ is an integral matrix and R_1 runs over the primitive representations of every such matrix by A.*

If $k = 1$, this amounts to the observation that all integral solutions t of $f(t_1, \ldots, t_n) = b_1$ are given by $t = \mu\mathfrak{x}$, where μ^2 is a square factor of b_1 and $\mathfrak{x}$ is a primitive solution of $f(x_1, \ldots, x_n) = b_1/\mu^2$.

It should be noted that, in finding or enumerating the representations of B_1 by A, either can be replaced by an equivalent matrix. If A is replaced by $P^T A P$ and B_1 by $V^T B_1 V$ where P and V are unimodular, then the representation T_1 is replaced by the corresponding representation $P^{-1} T_1 V$ of $V^T B_1 V$ by $P^T A P$.

It can be proved that the integral matrix T_1 has a *greatest right divisor* M, namely an integral non-singular matrix $M^{(k,k)}$ such that (*a*) $T_1 = R_1 M$ for some integral matrix R_1, and (*b*) if $N^{(k,k)}$ is any integral matrix such that $T_1 N^{-1}$ is integral, then MN^{-1} is integral. More generally, the following result holds.

LEMMA 3. *Let $T_1^{(n,k)}$ be an integral matrix of rank k, and denote the g.c.d. of the minor determinants of order k in T_1 by μ. Assume $1 \leq k < n$. Then,* (i) *T_1 has a greatest right divisor M,* (ii) *$|M| = \pm\mu$,* (iii) *every greatest right divisor of T_1 is given by VM, where $V^{(k,k)}$ is unit-modular,* (iv) *there exists an integral matrix $T_2^{(n,n-k)}$, called a (right) complement of T_1, such that $(T_1\ T_2)$ has determinant μ,* (v) *if T_2 is a particular complement of T_1, then every complement T^*_2 of T_1 is given by*

$$T^*_2 = T_1 H + T_2 U, \tag{6}$$

where $U^{(n-k,n-k)}$ is an arbitrary unimodular matrix and $H^{(k,n-k)}$ is any rational matrix such that $T_1 H$ (or MH) is integral.

It should be remarked that (i), (ii), and (iii) hold also when $k = n$. For the proof we refer to Siegel [10]. However, a proof of (v) for the primitive case will be useful later:

LEMMA 4. *If T_1 is primitive, and T_2 is one matrix such that $(T_1 T_2)$ is unimodular, then the most general such complement T^*_2 is given by* (6) *with U any $(n-k, n-k)$ unimodular matrix and H any $(k, n-k)$ integral matrix.*

Proof. Let $(S_1 S_2)^T$, with $S_1^{(n,k)}$ and $S_2^{(n,n-k)}$, denote $(T_1 T_2)^{-1}$. Then

$$S^T_1 T_1 = I_1,\quad S^T_1 T_2 = 0,\quad S^T_2 T_1 = 0,\quad S^T_2 T_2 = I_2, \tag{7}$$

where I_1 and I_2 denote identity matrices, of orders k and $n - k$. Hence, if T^*_2 is any complement of T_1,

$$\begin{bmatrix} S^T_1 \\ S^T_2 \end{bmatrix} (T_1 T^*_2) = \begin{bmatrix} I_1 & H \\ 0 & U \end{bmatrix}, \tag{8}$$

where $H = S^T_1 T^*_2$ and $U = S^T_2 T^*_2$. Evidently, H is integral and (comparing determinants) U is unimodular. Multiplying on the left by $(T_1 T_2)$, we have

$$(T_1\ T^*_2) = (T_1\ T_2)R, \text{ where } R = \begin{bmatrix} I_1 & H \\ 0 & U \end{bmatrix}, \tag{9}$$

and hence (6).

3. The basic algorithm. Let T_1 be a primitive representation of B_1 by A, $1 \leq k < n$. Choose a particular complement T_2 of T_1, so that $T = (T_1\ T_2)$ is unimodular, and construct the matrix equivalent to A,

$$B = T^{\mathsf{T}} AT = \begin{bmatrix} T^{\mathsf{T}}_1 AT_1 & T^{\mathsf{T}}_1 AT_2 \\ T^{\mathsf{T}}_2 AT_1 & T^{\mathsf{T}}_2 AT_2 \end{bmatrix} = \begin{bmatrix} B_1 & K^{\mathsf{T}} \\ K & B_2 \end{bmatrix}, \tag{10}$$

K and B_2 being defined by the last equation. Construct also $S^{\mathsf{T}} = T^{-1}$, $S = (S_1\ S_2)$, where $S_1^{(n,k)}$ and $S_2^{(n,n-k)}$, denote adj A by C, and construct

$$D = \text{adj } B = S^{\mathsf{T}} CS = \begin{bmatrix} S^{\mathsf{T}}_1 CS_1 & S^{\mathsf{T}}_1 CS_2 \\ S^{\mathsf{T}}_2 CS_1 & S^{\mathsf{T}}_2 CS_2 \end{bmatrix} = \begin{bmatrix} D_1 & L^{\mathsf{T}} \\ L & D_2 \end{bmatrix}. \tag{11}$$

The algorithm is based on a consideration of what happens to B (or D) when T_2 is replaced by other complements $T_1H + T_2U$ (H integral, U unimodular) of T_1.

Denote $|B_1|$ and $|D_2|$, respectively, by b_1 and d_2. It will be convenient to record here the result of "completing squares" relative to B_1 and D_2, in B and D. To complete squares, we replace B by $\mathrm{P}^{\mathsf{T}}BP$ and D by $Q^{\mathsf{T}}DQ$, where

$$P = \begin{bmatrix} I_1 & -B_1^{-1}K^{\mathsf{T}} \\ 0 & I_2 \end{bmatrix},\ Q = \begin{bmatrix} I_1 & 0 \\ -D_2^{-1}L & I_2 \end{bmatrix},\ PQ^{\mathsf{T}} = Q^{\mathsf{T}}P = I;$$

and so obtain

$$P^{\mathsf{T}}BP = \begin{bmatrix} B_1 & 0^{\mathsf{T}} \\ 0 & b_1^{-1}G \end{bmatrix},\ Q^{\mathsf{T}}DQ = \begin{bmatrix} d_2^{-1}E & 0^{\mathsf{T}} \\ 0 & D_2 \end{bmatrix}, \tag{12}$$

where

$$G = b_1B_2 - K(\text{adj } B_1)K^{\mathsf{T}},\ E = d_2D_1 - L^{\mathsf{T}}(\text{adj } D_2)L. \tag{13}$$

If $a = |A|$, then $|D| = a^{n-1}$, and it will be found that, since $BD = aI$,

$$L^{\mathsf{T}} = -B_1^{-1}K^{\mathsf{T}}\ D_2,\ GD_2 = ab_1I_2,\ B_1E = ad_2I_1,\ d_2 = b_1a^{n-k-1}, \tag{14}$$
$$|G| = ab_1^{n-k-1},\ \text{adj } G = b_1^{n-k-2}D_2,\ E = a^{n-k}\ \text{adj } B_1.$$

If T_2 is replaced by $T_1H + T_2U$, then T is replaced by TR, where

$$R = \begin{bmatrix} I_1 & H \\ 0 & U \end{bmatrix} = \begin{bmatrix} I_1 & 0 \\ 0 & U \end{bmatrix}\begin{bmatrix} I_1 & H \\ 0 & I_2 \end{bmatrix}. \tag{15}$$

Thus, the effect on the quadratic form $\mathfrak{x}^{\mathsf{T}} B\mathfrak{x}$, of replacing T_2 by $T_1H + T_2U$, is to apply the unimodular transformation U to the variables $x_{k+1}, \ldots, x_n$, and then the translation

$$x_i = y_i + \sum_{j=k+1}^{n} h_{ij}x_j (i = 1, \ldots, k),\ x_j = y_j (j = k+1, \ldots, n) \tag{16}$$

where $H = (h_{ij})$. The matrix G obtained by completing squares is evidently not affected by the translation (16). We thus have the following theorem.

THEOREM 1. *With any primitive representation T_1 of B_1 by A is associated an aggregate of pairs of matrices*:

$$U^{\mathsf{T}} GU \text{ and } U^{\mathsf{T}} K + H^{\mathsf{T}} B_1, \tag{17}$$

the aggregate being derivable from any one pair G and K by use of an arbitrary unimodular U and integral H. Here G is the matrix obtained on "completing squares" with respect to B_1, in the matrix $B = T^{\mathsf{T}} AT$, where T is a unimodular matrix having T_1 as its first k columns. The same matrices G and K are associated with WT_1, where W is any unimodular automorph of A.

The last statement is evident, since, if T is replaced by WT, the same matrices B and hence the same matrices G and K are obtained.

The important case $k = 1$ is worth formulating separately.

THEOREM 2. *Let* t *be a primitive representation of a non-zero number m by a real non-singular quadratic form f. All forms $g = mx_1^2 + \ldots$ obtained from f by unimodular transformations whose first column is* t, *are obtainable from any particular one of them,*

$$g_1 = m(x_1 + \ldots)^2 + \phi(x_2, \ldots, x_n), \tag{18}$$

of which the form after completing squares is here displayed, by applying an arbitrary unimodular transformation to ϕ, and then replacing x_1 by $x_1 + h_2x_2 + \ldots + h_nx_n$ with integers $h_2, \ldots, h_n$. The same forms g are obtained if t *is replaced by Wt, where W is a unimodular automorph of f.*

The invariance of the class of ϕ for a given primitive set of representations of m has important consequences in the theory of reduction of n-ary quadratic forms. It may be remarked also that there are applications in cosmogony of results of the sort that there is only one set of representations of certain numbers m, as for example [15] of 1 by $x^2 - y^2 - z^2 - t^2$; and this is connected (as will be clear from the following) with the fact that only one class of forms ϕ may appear on completing squares.

Conversely, for given B_1, G, and K, we can set

$$G + K(\text{adj } B_1)K^T = b_1B_2, \quad B = \begin{bmatrix} B_1 & K^T \\ K & B_2 \end{bmatrix}. \tag{19}$$

Observe that if G and K are replaced by $U^T GU$ and $U^T K + H^T B_1$, then B is replaced by $R^T BR$ with R as displayed in (9). If it *happens* that $A \sim B$, let T be a unimodular transformation of A into B. Then, as is well known, the most general such transformation is WT, where W ranges over the unimodular automorphs of A. Hence the matrices WT_1, where T_1 consists of the first k columns of T, constitute a set (WT_1) of primitive representations of B_1 by A associated with the pair G and K.

By confining attention to integral matrices A and B_1, some limitation is obtained on the possible matrices G and K. Then K and G are integral matrices such that

$$K(\text{adj } B_1)\, K^T \equiv -G \pmod{b_1}, \qquad (b_1 = |B_1|). \tag{20}$$

Since $B_1(\text{adj } B_1) = b_1I_1$, evidently if K satisfies (20), all the matrices $K + H^TB_1$ with $H^{(k,\,n-k)}$ an integral matrix, are also solutions. These matrices are said to form a *right-sided residue class modulo* B_1, and two matrices in the same right-sided residue class will be termed *congruent modulo* B_1 (or *right-congruent*, to avoid ambiguity).

If a matrix G is chosen in the class of equivalent matrices $U^T GU$, then U is restricted to be a unimodular automorph of G, and the associated matrices K satisfying (20) constitute a *complex of solutions of* (20), in accordance with the following definition. Two integral matrices K and K' are said to be in the same complex of solutions of (20) if, for some unimodular automorph U of G, $U^T K$ and K' are congruent modulo B_1.

Thus, every set (WT_1) of primitive representations of B_1 by A is uniquely associated with a certain class of matrices G, and if we select a matrix G of the class, with a unique complex of solutions K of (20). Conversely, any symmetric matrix G and associated complex of solutions of (20) is connected with a set of primitive representations of B_1 by some matrix A'.

In some cases, a set of nonequivalent matrices $A', \ldots, A^{(h)}$ and a set of nonequivalent matrices $G', \ldots, G^{(s)}$, each $G^{(j)}$ $(j = 1, \ldots, s)$ being accompanied by one or more complexes of solutions K of (20) with $G = G^{(j)}$, can be associated by our algorithm. For example, if $A', \ldots, A^{(h)}$ consist of representatives (one from each class) of a given determinant a, then (cf. (14)) $G', \ldots, G^{(s)}$ will be matrices of determinant ab_1^{n-k-1}; and if K is a solution of (20) with G one of the $G^{(j)}$, then the matrix B constructed as in (19) will have determinant a, and hence must be equivalent to one of $A', \ldots, A^{(h)}$. Examples will show that the matrices $G', \ldots, G^{(s)}$ may not comprehend all classes of determinant ab_1^{n-k-1}, since (20) may not be solvable for some of these. An important case is that where $A', \ldots, A^{(h)}$ are representatives of the classes of a genus. Then $G', \ldots, G^{(s)}$ can be shown to consist of the classes of one or more genera. In general, not every complex of solutions of K of (20) with $G = G^{(j)}$ will be such that the matrices B constructed therefrom as in (19) are in a prescribed genus, and it becomes necessary to specify those solutions.

It should be noted that, if $k = n - 1$, G is a matrix of one element, namely $ab_1^{n-k-1} = a = |A|$. The only unimodular automorph of G is $U = [1]$. Congruence (20) is then a single quadratic congruence

$$\sum_{i,j=1}^{n-1} c_{ij} k_i k_j \equiv -a \pmod{b_1}, \tag{21}$$

where adj $B_1 = (c_{ij})$ and $K = [k_1, k_2, \ldots, k_{n-1}]$. Accordingly, all the primitive representations of an $(n-1)$-ary quadratic form by an n-ary quadratic form f can be found by solving (21), constructing from these solutions quadratic forms g with matrix B as in (19), and determining whether f is equivalent to such forms g.

This process is somewhat simpler than that of Gauss, Smith, and Minkowski, who preferred to work with the adjoint form (11), as will be briefly indicated in § 9. If the matrices G are known, the process can be used for $n - k > 1$.

4. A fundamental quantitative relation. The preceding association can be put on a more quantitative basis by use of the following theorem.

THEOREM 3. *Let A, T_1, B_1, G, and K be associated as in the preceding algorithm. Let $\Gamma_1(A, T_1)$ denote the subgroup of unimodular automorphs W of A such that $WT_1 = T_1$, and $\Gamma_2(G, K)$ the subgroup of unimodular automorphs U of G such that $U^T K$ and K are congruent modulo B_1. The two subgroups are isomorphic.*

Proof. If T is unimodular and T_1 is the matrix of its first k columns, and $B = T^{\mathsf{T}} AT$, then the most general unimodular transformation of A into B with T_1 the matrix of its first k columns is given by WT with W in $\Gamma_1(A, T_1)$. For every such W, $T^{-1}WT$ is an automorph of B of the special form

$$T^{-1}WT = T^{-1}(T_1 \;\; WT_2) = R = \begin{bmatrix} I_1 & H \\ 0 & U \end{bmatrix}. \tag{22}$$

The condition $R^{\mathsf{T}} BR = B$ expands into

$$K = U^{\mathsf{T}} K + H^{\mathsf{T}} B_1, \;\; U^{\mathsf{T}} GU = G. \tag{23}$$

Hence U belongs to $\Gamma_2(G, K)$. Conversely, if U is in $\Gamma_2(G, K)$, and H is defined by (23_1), then $R^{\mathsf{T}} BR = B$ for the R displayed in (22), and $W = TRT^{-1}$ is an automorph of A such that $WT_1 = TR(I_1\, 0)^{\mathsf{T}} = (T_1\, T_2)(I_1\, 0)^{\mathsf{T}} = T_1$. This sets up a one-one correspondence between the two subgroups, and is it easily verified that this correspondence is preserved under multiplication.

COROLLARY. *If $k = n - 1$, the representations WT_1 of a set are different for different automorphs W, and the only automorph W of A such that $WT_1 = T_1$ is $W = I$.*

Proof. The matrix G is unary and the only U is [1]. Note the assumption here that A and B_1 are non-singular.

The number ν of elements in $\Gamma_2(G, K)$ may be finite or infinite, but the index denoted by γ, of $\Gamma_2(G, K)$ within the group $\Gamma_2(G)$ of all unimodular automorphs U of G, is finite. Indeed, if the elements of $\Gamma_2(G, K)$ are denoted by U', U'', . . . , then each coset $U'V$, $U''V$, . . . is characterized by the property that the products $V^{\mathsf{T}} U'^{\mathsf{T}} K$, $V^{\mathsf{T}} U''^{\mathsf{T}} K$, . . . , are congruent modulo B_1; and the number of incongruent residues modulo B_1 is finite. Thus γ is equal to the number of incongruent elements K modulo B_1 in a complex of solutions of (20). If the number u of automorphs U of G is finite, $u = \nu\gamma$. Hence, by Theorem 3, if also the number w of automorphs W of A is finite,

$$\frac{1}{\nu} = \frac{\textit{number of distinct representations } WT_1}{w} = \frac{\gamma}{u}. \tag{24}$$

If w is finite, the *weight of a representation* T_1 *(by* A*)* is defined to be $1/w$. By (24), the sum of the weights of the representations in a set (WT_1) is $1/\nu$. Now ν is finite when u is finite, even though w may be infinite. It is consistent and natural to define the *weight of a set of representations* (WT_1) to be $1/\nu$, if ν is finite.

The association of § 3 can therefore be given the following quantitative form. Let the numbers u_j of unimodular automorphs of $G^{(j)}$ be assumed finite, $(j = 1, \ldots, s)$. Denote by $A^{(i)}(B_1)$ the sum of the weights of all sets of primitive representations of B_1 by $A^{(i)}$; and let $\rho(G^{(j)})$ denote the number of solutions K of (20) (with $G = G^{(j)}$) which are incongruent modulo B_1 and are such that the corresponding matrix B in (19) is equivalent to one of the $A^{(i)}$. Then

$$\sum_{i=1}^{h} A^{(i)}(B_1) = \sum_{j=1}^{s} \rho(G^{(j)})/u_j. \tag{25}$$

Note that if $A^{(i)}[B_1]$ denotes the number of primitive representations of B_1 by

$A^{(i)}$, and the numbers $w_1, \ldots, w_h$ of unimodular automorphs of $A', \ldots, A^{(h)}$ are finite, the left member of (25) has the form $\Sigma A^{(i)}[B_1]/w_i$.

The *weight of a matrix*, or class, is the reciprocal of the number of its unimodular automorphs. Hence the right member of (25) is the sum of the weights of the matrices $G^{(j)}$ multiplied by $\rho(G^{(j)})$. Since matrices of a given genus can be supposed congruent to any modulus, $\rho(G^{(j)})$ depends only on the genus of $G^{(j)}$. Hence, if the matrices $G^{(j)}$ include the classes of a genus τ, and $\rho(\tau)$ denotes the value of $\rho(G)$ for G in τ, the corresponding terms in (25) unite into $\rho(\tau)w(\tau)$ where $w(\tau)$ denotes the weight of the genus, *i.e.* the sum of weights of its classes.

5. An example: representation by binary quadratic forms, $n = 2$, $k = 1$. The reader may find it of interest to review this classical case as an instance of the preceding methods. Let $f = [a, b, c]$ denote an integral binary quadratic form of non-zero discriminant $d = b^2 - 4ac$. It is desired to find the primitive representations $\mathfrak{x}$ of a given non-zero integer m by f, *i.e.* the coprime solutions x_1, x_2 of

(a) $$ax_1^2 + bx_1x_2 + cx_2^2 = m.$$

If $\mathfrak{x}$ is a primitive solution of (a), there exist integers y_1, y_2 such that $x_1y_2 - x_2y_1 = 1$; and it is easily seen that the general formula for such integers is given in terms of a particular pair by $y_1 + hx_1$, $y_2 + hx_2$, with h an arbitrary integer. The unimodular $T = [\mathfrak{x}\ \mathfrak{y}]$ replaces f by $g = [m, n, q]$ where

(b) $$n = 2ax_1y_1 + b(x_1y_2 + x_2y_1) + 2cx_2y_2,$$

m is given by (a), and q is then fixed by the discriminant $d = n^2 - 4mq$. If y_1 and y_2 are replaced by $y_1 + hx_1$ and $y_2 + hx_2$, g is replaced by the equivalent form $[m, n + 2hm, q']$. Thus, every primitive representation $\mathfrak{x}$ of m by f is associated with a solution $z = n$ of

(c) $$z^2 \equiv d \pmod{4m}, \quad 0 \leq z < |2m|.$$

For any unimodular automorph W of f, WT replaces f by the same g, and the set of primitive representations $W\mathfrak{x}$ is associated with the same root z of (c).

Conversely, for every solution z of (c), consider the integral form

(d) $$g_z = [m, z, (z^2 - d)/(4m)], \text{ of discriminant } d.$$

If f is not equivalent to g_z, then no primitive representations of m by f are associated with z. If $f \sim g_z$, and T is a unimodular transformation of f into g_z, the most general such transformation is WT, W ranging over the unimodular automorphs of f. The first columns $W\mathfrak{x}$ of WT constitute a set of primitive representations of m by f associated with z. Hence we have two theorems:

THEOREM A (Gauss). *Let $f = [a, b, c]$ be an integral binary quadratic form of non-zero discriminant d, m be a non-zero integer. The number $f'(m)$ of primitive sets of representations of m by f is equal to the number of solutions z of* (c) *such that $f \sim [m, z, (z^2 - d)/(4m)]$.*

THEOREM B (Dirichlet). *Let $f_1, \ldots, f_h$ be representative forms, one from each class, of integral binary quadratic forms of a given non-zero discriminant d, m be*

a non-zero integer. Let $R'(m, d)$ denote the number $f'_1(m)+\ldots+f'_h(m)$ of sets of primitive representations of m by the system of forms $f_1, \ldots, f_h$. Then $R'(m, d)$ equals the number of solutions z of (c).

If we desired the number of sets of primitive representations of m by the system of *primitive* classes of discriminant d, we would merely restrict z to be a solution of (c) such that g_z is primitive. Or, if we wished the classes to be those of a given genus, we could express the condition that g_z is in that genus. It is readily shown that if m is divisible by no prime p such that d/p^2 is an integer of the form $4k + 0$ or 1, then m is represented in at most one genus of discriminant d, and that g_z is necessarily primitive,—so that both the preceding conditions are somewhat trivial in the binary case.

6. The primitive representation of a binary quadratic form as a sum of three squares. As a preliminary to its extension in § 8, we consider by the preceding methods the classic problem of finding the number N of primitive representations of a positive-definite classic binary quadratic form $\phi = [a', 2t', b']$ by $x^2+ y^2 + z^2$, that is the number of solutions of the identity

$$a'x^2+ 2t'xy + b'y^2=(\alpha_1 x + \beta_1 y)^2+(\alpha_2 x + \beta_2 y)^2+(\alpha_3 x + \beta_3 y)^2$$

in integers $\alpha_1, \ldots, \beta_3$ such that $\alpha_2\beta_3- \alpha_3\beta_2$, $\alpha_1\beta_2- \alpha_2\beta_1$, $\alpha_3\beta_1- \alpha_1\beta_3$ are relatively prime. Here $A = I^{(3,3)}$, B_1 is the matrix of ϕ, $b_1= a'b'- t'^2 >0$, and (21) reduces to

$$b'k_1^2 - 2t'k_1k_2+ a'k_2^2 \equiv -1 \pmod{b_1}, \tag{26}$$

with $K = [k_1, k_2]$. For any integral solution K of (26), the matrix

$$B = \begin{bmatrix} B_1 & K^{\mathrm{T}} \\ K & B_2 \end{bmatrix}, \text{ where } B_2=(1 + b'k_1^2- 2t'k_1k_2+ a'k_2^2)/b_1,$$

is a classic, positive-definite matrix of determinant 1, and hence (since there is only one class of such matrices) is equivalent to A. Since A has 24 unimodular automorphs and $G = [1]$, $N=24\lambda$, where λ is the number of solutions K modulo B_1 of (26). The computation of λ is reduced to that of the number μ of solutions K modulo b_1, by the following lemma.

LEMMA 5. *Let $B_1^{(k,k)}$ be assumed merely integral and of non-zero determinant $\pm\beta$, $\beta > 0$. Set $H^{\mathrm{T}} = [h_1, \ldots, h_k]$. As $h_1, \ldots, h_k$ run through all integers, $H^{\mathrm{T}} B_1$ gives rise to exactly β^{k-1} incongruent matrix residues modulo β.*

Proof. The property in question is unaltered if B_1 is multiplied on both sides by unit-modular matrices. Hence B_1 can be replaced by a diagonal matrix $\{e_1, \ldots, e_k\}$, where the e's are positive integers and their product equals β. Then $H^{\mathrm{T}} B_1$ is the diagonal matrix $\{h_1e_1, \ldots, h_ke_k\}$, and the elements have, independently, $\beta/e_1, \ldots, \beta/e_k$ residues modulo β.

Now μ/λ is equal to the number of incongruent residues modulo b_1 which are obtained, for given K, from $K + H^{\mathrm{T}} B_1$ as $H^{\mathrm{T}} = [h_1, h_2]$ ranges over all integral vectors. By Lemma 5, $\mu/\lambda = b_1$. Hence $N = 24\ \mu/b_1$.

The conditions for (26) to be solvable (and hence for ϕ to be primitively representable as a sum of three squares) will now be examined. No odd prime p can divide all three numbers a', t', and b', since such a prime would divide the

modulus b_1 and does not divide the right member -1. Similarly, if a' and b' are even, then t' must be odd, hence $b_1 \equiv 3 \bmod 4$. Since, by (26), ϕ represents $-1 \bmod p$, the generic character $(\phi|p)$ must have the value $(-1|p)$ for every odd prime p dividing b_1. Now, if ϕ_1 is any primitive non-negative binary quadratic form of discriminant d $(= -2^q e,\ e \text{ odd},\ q \geq 0)$, then the generic characters of ϕ_1 are known to satisfy

$$(27) \qquad (2|m)^q(-1|m)^{\frac{1}{2}(e+1)} \prod_{i=1}^{s} (m|p_i) = 1,$$

where $|e| = p_1 p_2 \ldots p_s$ expresses $|e|$ as a product of primes, and m denotes any integer prime to d and represented by ϕ_1. If $b_1 \equiv 4$ or $0 \bmod 8$, the residue mod 4 or 8 of the odd numbers represented by ϕ is invariant, and by (26) this residue has to be that of -1; however, if we substitute -1 for m in (27), it reduces to the impossibility $(-1)^{\frac{1}{2}(e+1)}\ (-1)^{\frac{1}{2}(e-1)} = 1$. Hence $b_1 \not\equiv 0 \bmod 4$. The same contradiction is found if ϕ is properly primitive and $e = b_1 \equiv 3 \bmod 4$. Finally, if ϕ is improperly primitive (hence $b_1 \equiv 3 \bmod 4$), then the application of (27) to $\phi_1 = \frac{1}{2}\phi$, for which $(\phi_1|p) = (-2|p)$, shows that $(2|b_1) = -1$, *i.e.* $b_1 \equiv 3 \bmod 8$. Hence, *a positive definite classic binary quadratic form is primitively representable as a sum of three squares if and only if ϕ is p.p. and $|\phi| \equiv 1$ or $2 \bmod 4$, or ϕ is i.p. and $|\phi| \equiv 3 \bmod 8$, and ϕ represents $-1 \bmod |\phi|$.*

Now a form equivalent to ϕ can be given the residue $ax^2 + hb_1y^2 \bmod b_1$, where $a \equiv -1 \equiv h \bmod b_1$. Hence (26) has $2^\nu b_1$ solutions, and $N = 24.2^\nu$, where ν denotes the number of distinct odd primes dividing b_1.

To obtain the number of primitive representations of a positive integer b_1 $(\equiv 1$ or $2 \bmod 4$, or $3 \bmod 8)$ as a sum of three squares, we may take $n = 3$, $k = 1$, $A' = I$, $h = 1$, $B_1 = b_1$ in (25). Then $G', \ldots, G^{(s)}$ are representative matrices (one from each class) of the particular genus of binary quadratic forms of determinant b_1 which are primitively representable by adj I $(= I)$. Using the residue $-x^2 - b_1y^2 \bmod b_1$ for any of the $G^{(i)}$, (20) becomes

$$\begin{bmatrix} k_1^2 & k_1k_2 \\ k_2k_1 & k_2^2 \end{bmatrix} \equiv -\begin{bmatrix} -1 & 0 \\ 0 & 0 \end{bmatrix} \pmod{b_1},$$

which has 2^ν solutions $k_1, k_2 \bmod b_1$. Hence, the number of primitive representations of b_1 as a sum of three squares is equal to $24.2^\nu\, s/u$, where s denotes the number of classes of the genus described above, and u is the number of unimodular automorphs of any form in that genus ($u = 4$ if $b_1 = 1$, $u = 6$ if $b_1 = 3$, $u = 2$ otherwise.)

7. Properties of Hermite-matrices. To obtain all representations, primitive or imprimitive, of B_1 by A, we have to consider the Hermite-matrices M such that $M^{T^{-1}} B_1 M^{-1}$ is in a genus capable of primitive representation by A. The discussion will be simplified by reduction to the case where $|M|$ is a power of a prime.

LEMMA 6. (i) *Let m_1, m_2 be coprime integers. An integral matrix Q of determinant m_1m_2 has a unique Hermite-matrix of determinant m_2 as a right-divisor.* (ii) *If $m_1, m_2, \ldots, m_s$ are coprime in pairs, a matrix Q of determinant*

$m_1m_2 \ldots m_s$ can be expressed in one and only one way in the form $UM'_1M'_2, \ldots, M'_s$, where U is unimodular and $M'_1, \ldots, M'_s$ are Hermite-matrices of respective determinants $m_1, \ldots, m_s$. (iii) *If $M_1, \ldots, M_s$ are Hermite-matrices of determinants $m_1, \ldots, m_s$, coprime in pairs, then the matrix Q of determinant $m_1m_2 \ldots m_s$ having M_i as its right-divisor of determinant m_i $(i = 1, \ldots, s)$ is uniquely determined up to a left-unimodular factor. Hence, if Q is a Hermite-matrix, it is unique.*

Proof. (i) We can express U_1QU_2 as a diagonal matrix D, which can evidently be factored as D_1D_2 with $|D_1| = m_1$ and $|D_2| = m_2$. The existence of a right-divisor of Q, with determinant m_2 follows. This divisor can be supposed to be an Hermite-matrix. To establish its uniqueness, consider $N_1M_1 = N'_1M'_1$, where $|N_1| = |N'_1| = m_1$, and $|M'_2| = |M_2| = m_2$. Hence $(N'_1)^{-1}N_1 = (M'_2M_2^{-1})$, and both sides are integral since their respective possible denominators are coprime. Hence $M'_2 = UM_2$ with U unimodular, and $U = I$ by Lemma 2.

(ii) Obvious by repeated applications of (i).

(iii) Let $Q = Q_1M_1$. We will prove that the Hermite right-divisors of Q_1 with the determinants $m_2, \ldots, m_s$ are uniquely determined, and hence (iii) will follow by induction. Thus, suppose $Q_2M'_2M_1 = Q_2N_1M_2$ and $Q_4M''_2M_1 = Q_3N'_1M_2$, where the Q's have determinants $m_3, \ldots, m_s$ and the other matrices have determinants m_1 or m_2 according to their subscripts. The argument used in (i) shows that $M'_2M_1 = UN_1M_2$ and $M''_2M_1 = U'N'_1M_2$. Hence $(UN_1)^{-1}M'_2 = (U'N'_1)^{-1}M''_2$, $(UN_1)(U'N'_1)^{-1}$ must be integral and hence unimodular, $M'_2 = U''M''_2$, $M'_2 = M''_2$.

Two quadratic forms are in the same genus if they have the same index and and determinant, and are in the same class w.r.t. p (defined by residues modulo p^r with r large) for every prime p dividing the determinant and for the prime 2. The class w.r.t. p is unchanged by the application to the quadratic form of integral transformations of determinants prime to p, or of rational transformations of determinants prime to p and with coefficients whose denominators are prime to p. It follows that the class w.r.t. p of $B''_1 = (M^{\mathsf{T}})^{-1}B_1M^{-1}$ is the same as that of $(M^{\mathsf{T}}_1)^{-1}B_1M_1^{-1}$, where M_1 is the Hermite right-divisor of M whose determinant is the highest power of p dividing $|M|$. Also, by (iii) of Lemma 6, the number of Hermite-matrices of determinant $m_1m_2 \ldots m_s$ (where the m_i are powers of distinct primes p_i, $i = 1, \ldots, s$) for which $(M^{\mathsf{T}})^{-1}B_1M^{-1}$ is in a given genus, is the product of the numbers of Hermite-matrices M_i of determinant m_i for which $(M^{\mathsf{T}}_i)^{-1}B_1M_i^{-1}$ is in the class w.r.t. p_i determined by that genus.

Let B_1 be an integral, positive-definite 2 by 2 matrix of determinant b_1, and let ν denote the number of distinct odd primes dividing b_1. Let $\chi(p)$ denote the number of Hermite-matrices

$$M_1 = \begin{bmatrix} p^r & q \\ 0 & p^s \end{bmatrix}, \quad q, r, \text{ and } s \text{ non-negative integers, } q < p^s, \tag{28}$$

such that $B'_1=(M^{\mathsf{T}}{}_1)^{-1}B_1M_1^{-1}$ is an integral matrix satisfying the conditions of primitive representation by $x^2+y^2+z^2$ relating to the prime p, but if $p>2$ count every system q, r, s for which $|B'_1|$ is prime to p as worth only $\frac{1}{2}$. The reason for counting the latter systems as worth $\frac{1}{2}$ is that in applying the formula 24.2^r for the number of primitive representations of B'_1 (or rather of B''_1) by I, the value of ν is diminished by one, from the value as defined for B_1. Accordingly, the number of all representations of B_1 by $I^{(3,3)}$ will be

$$24.2^r\prod_p\chi(p),$$

where p runs over the primes such that $p^2|4b_1$.

8. The factors $\chi(p)$. First consider $p>2$. The form ϕ can be given the residue $p^{u_1}m_1x_1^2+p^{u_2}m_2x_2^2 \pmod{p^\tau}$ (τ sufficiently large), where m_1 and m_2 are prime to p, and $0\le u_1\le u_2$. On applying to ϕ the inverse of (28), we obtain the form

$$\phi'=a_1x_1^2+2b_1x_1x_2+c_1x_2^2,\quad a_1=p^{u_1-2r}m_1,\quad b_1=-qp^{u_1-2r-s}m_1,$$
$$c_1=p^{-2r-2s}(q^2p^{u_1}m_1+p^{2r+u_2}m_2). \tag{29}$$

The conditions on ϕ' for primitive representability by $x^2+y^2+z^2$ are that one of a_1, b_1, c_1 be prime to p, and that if p divides $|\phi'|$ then ϕ' must represent $-1 \bmod p$. It will be convenient to consider instead the slightly more general condition that ϕ' shall represent $-d \bmod p$, where d is a given integer prime to p.

The solutions with a_1 prime to p require

$$r=\tfrac{1}{2}u_1,\ q=0,\ s\le\tfrac{1}{2}u_2, \tag{30}$$

since b_1 and c_1 must be integers and $q<p^s$. With $q=0$, we may have also

$$r<\tfrac{1}{2}u_1,\ q=0,\ s=\tfrac{1}{2}u_2, \tag{31}$$

since c_1 must be prime to p when p divides a_1 and b_1. For the remaining cases, with q not zero, we set $q=p^tq_1$, $0\le t<s$, q_1 prime to p.

If $p|a_1$ but not b_1, then $u_1+t=2r+s$, hence (c_1 being integral), $u_1+2t<2r+2s$, $u_1+2t=2r+u_2$. From these readily follow $u_2=t+s$, $\frac{1}{2}(u_2-u_1)\le t=u_2-s$, and hence

$$\tfrac{1}{2}u_2<s\le\tfrac{1}{2}(u_1+u_2),\ t=u_2-s,\ r=t-\tfrac{1}{2}(u_2-u_1). \tag{32}$$

Also, q_1 has $2e_3$ values mod $p^{2s-u_2}=p^{s-t}$, where $e_3=\frac{1}{2}\{1+(-m_1m_2|p)\}$; and hence q has $2e_3$ values mod p^s for each complex of values s, t, r. Note that in the present case $|\phi'|$ is prime to p.

There remain to be considered the cases satisfying

(33) $2r<u_1,\ 2r+s<u_1+t$, p^{2r+2s} *precisely divides* $p^{u_1+2t}q_1^2m_1+p^{2r+u_2}m_2$.

It will be convenient to subdivide these cases into three parts, as follows:

(a) $2s=u_2$, $\frac{1}{2}(u_2-u_1)<t<\frac{1}{2}u_2$, $r=t-\frac{1}{2}(u_2-u_1)$;

(b) $\frac{1}{2}u_2\le s<\frac{1}{2}(u_1+u_2)$, $\frac{1}{2}(u_2-u_1)\le t<u_2-s$, $r=t-\frac{1}{2}(u_2-u_1)$, *while* $q_1 \bmod p^{s-t}$ *is such that* $(q_1^2m_1+m_2)/p^{2s-u_2}$ *is prime to* p;

(c) $r<\frac{1}{2}u_1$, $t<r+\frac{1}{2}(u_2-u_1)$, $s=t+\frac{1}{2}u_1-r$, q_1 *arbitrary prime to* p.

Thus (a) can be verified as embodying the conditions to be satisfied when $2r + 2s = 2r + u_2 < 2t + u_1$, whence (as $r \geq 0$) $\frac{1}{2}(u_2 - u_1) < t < s$. Again, (b) corresponds to $u_1 + 2t = u_2 + 2r \leq 2r + 2s$, whence (by (33_2)) $t < u_2 - s \leq \frac{1}{2}u_2$. Note here, for use in the case where $2s = u_2$, that it can be proved that $q_1^2 m_1 + m_2$ has the quadratic character of $-d$ modulo p for precisely θ values q_1 modulo p, where

$$\theta = \tfrac{1}{2}\{p - 2 - (-dm_1|p) - (-dm_2|p) - (-m_1m_2|p)\}. \tag{34}$$

Note also that if $2s > u_2$, $(-m_1m_2|p) = 1$, and $q_1^2 m_1 + m_2 = p^{2s-u_2}q'$, then

$$(q_1 + hp^{2s-u_2})^2 m_1 + m_2 = p^{2s-u_2}(q' + 2q_1m_1h + p^{2s-u_2}h^2m_1),$$

and the last factor has the quadratic character modulo p of $-d$ for $\frac{1}{2}(p-1)$ residues h modulo p; consequently, $(q_1^2m_1 + m_2)/p^{2s-u_2}$ has the quadratic character of $-d$ for $p-1$ residues q_1 modulo p^{2s-u_2+1}. Finally, (c) occurs if $u_1 + 2t = 2r + 2s < 2r + u_2$ (whence $t < s$ is equivalent to $r < \frac{1}{2}u_1$).

We will use the abbreviations $\epsilon_1, \epsilon_2, \epsilon_3 = 0$ or 1 according as (respectively) $u_1, u_2, u_2 - u_1$ are odd or even; and $\eta_i = \frac{1}{2}\{1 + (-dm_i|p)\}$, $\delta_i = \{\frac{1}{2}(u_i + 1)\}$, $(i = 1, 2)$; $\eta_3 = \frac{1}{2}\{1 + (-m_1m_2|p)\}$.

For odd p, $\chi(p)$ will be a sum of terms due to each of the cases (30) to (33) (c), and determined as follows.

If $2s < u_2$ in (30), m_1 must have the quadratic character of $-d$. Hence the terms $\chi(p)$ corresponding to (30) and (31) are, respectively,

$$\epsilon_1\delta_2\eta_1 + \tfrac{1}{2}\epsilon_1\epsilon_4, \text{ and } \epsilon_3\delta_1\eta_3, \tag{35}$$

the $\frac{1}{2}$ being due to the circumstance that $|\phi'|$ is prime to p if $s = \frac{1}{2}u_2$ in (30). The term of $\chi(p)$ arising from (32) is evidently

$$\epsilon_3\eta_3\delta_1. \tag{36}$$

In case (33)(a), for each value $t = \frac{1}{2}u_2 - i$ $(i = 1, 2, \ldots, \delta_1 - 1)$, q_1 has $(p-1)p^{s-t-1} = (p-1)p^{i-1}$ values modulo p^{s-t}, and r has $\delta_1 - i$ values. The corresponding part of $\chi(p)$ is therefore

$$\epsilon_2\eta_2 \sum_{i=1}^{\delta_1 - 1} (p-1)p^{i-1}(\delta_1 - 1) = \epsilon_2\eta_2\{(p^{\delta_1} - 1)/(p-1) - \delta_1\}. \tag{37}$$

If $2s = u_2$ in (33)(b), we can set $t = s - j$ $(j = 1, 2, \ldots, \frac{1}{2}u_1)$. Then q_1 has θp^{j-1} values modulo p^{s-t}, and the corresponding part of $\chi(p)$ is

$$\theta\epsilon_2\epsilon_3 \sum_j p^{j-1} = \tfrac{1}{2}\epsilon_2\epsilon_3(p^{\delta_1} - 1) - \zeta\epsilon_2\epsilon_3(p^{\delta_1} - 1)/(p-1), \tag{38}$$

where $\zeta = \frac{1}{2}\{1 + (-dm_1|p) + (-dm_2|p) + (-m_1m_2|p)\} = \eta_1 + \eta_2 + \eta_3 - 1$. If $2s > u_2$ in (33)(b), we can set $s = \frac{1}{2}(u_1 + u_2) - i$ $(i = 1, \ldots, \delta_1 - 1)$ and $t = \frac{1}{2}(u_2 - u_1) + j$ $(j = 0, 1, \ldots, i-1)$, and have for the corresponding term of $\chi(p)$,

$$\epsilon_3\eta_3 \sum_i \sum_j (p-1)p^{i-j-1} = \epsilon_3\eta_3\{(p^{\delta_1} - 1)/(p-1) - \delta_1\}. \tag{39}$$

Finally, in (33) (c), u_1 is even, and for given r, t, and s, q_1 has $(p-1)p^{s-t-1} = (p-1)p^{\delta_1 - r - 1}$ residues mod p^{s-t}, and the corresponding term of $\chi(p)$ is

$$\eta_1\epsilon_1 \sum_{r=0}^{\delta_1 - 1} (r - \delta_1 + \delta_2)(p-1)p^{\delta_1 - r - 1} = \eta_1\epsilon_1\{(\delta_2 - \delta_1)p^{\delta_1} + (p^{\delta_1} - 1)/(p-1) - \delta_1\}. \tag{40}$$

The sum of the terms in (35)-(40) will be found to be

$$\chi(p) = \kappa_1(p^{\delta_1} - 1)/(p-1) + \kappa_2 p^{\delta_1}, \tag{41}$$

where $\kappa_1 = \epsilon_1\eta_1 + \epsilon_2\eta_2 + \epsilon_3\eta_3 - (\eta_1 + \eta_2 + \eta_3 - 1)\epsilon_1\epsilon_2$, $\kappa_2 = \frac{1}{2}\epsilon_1\epsilon_2 + \epsilon_1\eta_1(\delta_2 - \delta_1)$. Thus the values of κ_1 and κ_2 may be tabulated as follows:

	κ_1	κ_2
Case u_1 even, u_2 even.	1	$\frac{1}{2} + \frac{1}{2}\{1 + (-dm_1\|p)\}(u_2 - u_1)/2$
u_1 even, u_2 odd.	$\frac{1}{2}\{1 + (-dm_1\|p)\}$	$\frac{1}{2}\{1 + (-dm_1\|p)\}u_2 + 1 - u_1)/2$
u_1 odd, u_2 even.	$\frac{1}{2}\{1 + (-dm_2\|p)\}$	0
u_1 odd, u_2 odd.	$\frac{1}{2}\{1 + (-m_1m_2\|p)\}$	0

The value of $2\chi(p)$ thus obtained agrees with that for the case $d = 1$ given by the author [8] without details of proof; the method then used was quite different and based on a formula of Siegel. To express the value of $\chi(p)$ in terms of generic characters of ϕ, we may write $\phi = k\phi_1$, where ϕ_1 is either p.p. or i.p., and k is a positive integer. For each odd prime p, we may set $k = p^{u_1}k_1$, and $|\phi_1| = p^{u_2-u_1}t_1$, where k_1 and t_1 are prime to p. Then u_1 and u_2 coincide with their values in the associated form-residue $p^{u_1}m_1x_1^2 + p^{u_2}m_2x_2^2$, $(m_1|p) = (k_1|p)(\phi_1|p)$, $(m_1m_2|p) = (t_1|p)$.

Before discussing $\chi(2)$, we will compute the modified value $\chi_1(p)$ for Linnik's problem, in which the number of representations is desired in which the divisor k of the binary form is equal to the divisor of the representations. This now means that $u_1 = r + s$.

In (30) this gives $r = s = \frac{1}{2}u_1$, and contributes to $\chi_1(p)$ the term $\epsilon_1\eta_1$ if $u_1 < u_2$, $\frac{1}{2}\epsilon_1\epsilon_2$ if $u_1 = u_2$. The contribution due to (31) is 0 unless $\frac{1}{2}u_2 \leq u_1 < u_2$, and then is $\epsilon_2\eta_2$. In (32), we need $u_1 = u_2$, and then get $\eta_3\delta_1$ values r, s, t. So far the contribution is small. However, in case (33)(a), if $r + s = u_1$, then $r = u_1 - \frac{1}{2}u_2 < t - \frac{1}{2}(u_2 - u_1)$, $t > \frac{1}{2}u_1$. Thus (33) (a) requires that $\frac{1}{2}u_2 \leq u_1 < u_2$, and the conditions to be satisfied are

$$\tfrac{1}{2}u_1 < t < \tfrac{1}{2}u_2,\ 2s = u_2,\ r = u_1 - s,\ q_1 \text{ prime to } p.$$

Thus we may set $t = \frac{1}{2}u_2 - i$, $(i = 1, 2, \ldots, v)$, where $v = [\frac{1}{2}(u_2 - u_1 - 1)]$, q_1 has $(p-1)p^{s-t-1} = (p-1)p^{i-1}$ values modulo p^{s-t}, r now has one value, and the corresponding part of $\chi_1(p)$ is

$$\epsilon_2\eta_2 \sum_i (p-1)p^{i-1} = \epsilon_2\eta_2(p^v - 1).$$

Case (33) (b) is found to require $\frac{1}{2}u_2 \leq u_1 < u_2$, and then to specify

$$\tfrac{1}{2}(u_2 - u_1) \leq t \leq \tfrac{1}{2}u_1,\ r = t - \tfrac{1}{2}(u_2 - u_1),\ s = \tfrac{1}{2}(u_1 + u_2) - t.$$

The subcase $2s = u_2$ implies $u_1 = 2t$ and gives the contribution $\theta\epsilon_1\epsilon_2 p^{\frac{1}{2}(u_2-u_1)-1}$. Also, $2s > u_2$ implies $t < \frac{1}{2}u_1$, we can set $t = \frac{1}{2}(u_2 - u_1) + j$ $(j = 0, 1, \ldots, u_1 - 1 - [\frac{1}{2}u_2])$, and find the contribution $\epsilon_3\eta_3(u_1 - [\frac{1}{2}u_2])(p-1)p^{\frac{1}{2}(u_2-u_1)-1}$. Finally, (33) (c) is equivalent to

$$\tfrac{1}{2}u_1 < s < \tfrac{1}{2}u_2,\ \ 0 \leq r = u_1 - s,\ t = \tfrac{1}{2}u_1.$$

Hence the contribution to $\chi_1(p)$ is

$$\eta_1\epsilon_1 \sum_{s=\frac{1}{2}u_1+1}^{u_1} (p-1)p^{s-\frac{1}{2}u_1-1} = \eta_1\epsilon_1(p^{\frac{1}{2}u_1} - 1) \text{ or } \eta_1\epsilon_1 \sum_{s=\frac{1}{2}u_1+1}^{[\frac{1}{2}(u_2-1)]} (p-1)p^{s-\frac{1}{2}u_1-1} = \eta_1\epsilon_1(p^v - 1),$$

according as $u_1 < \frac{1}{2}u_2$ or $\frac{1}{2}u_2 \leq u_1 < u_2$.

Summing up, the value of $\chi_1(p)$ for odd primes p is given by

$$(42)\qquad \begin{cases} 1, \text{ if } u_1 = u_2 = 0; \\ \tfrac{1}{2}\epsilon_1\epsilon_2 + \eta_3\delta_1, \text{ if } u_1 = u_2 > 0; \\ \eta_1\epsilon_1 p^{u_1/2}, \text{ if } u_1 < \tfrac{1}{2}u_2; \end{cases}$$

$p^v\rho$, if $\tfrac{1}{2}u_2 \leq u_1 < u_2$, where $\rho = \epsilon_1\eta_1 + \epsilon_2\eta_2 + \theta\epsilon_1\epsilon_2 + \epsilon_3\eta_3(u_1 - [\tfrac{1}{2}u_2])(p-1)$. Here $v = [\tfrac{1}{2}(u_2 - u_1 - 1)]$. Note that the order of size of this factor is that of the power of p dividing h, where h^2 is the largest square factor common to k and $|\phi_1|$.

Except for the values of $\chi(2)$ and $\chi_1(2)$, we have the following theorem.

THEOREM 4. *Let k be a positive integer, ϕ_1 be a positive-definite integral binary quadratic form, either properly or improperly primitive, $\Delta = |\phi_1| \neq 0$, $\phi = k\phi_1$. The number of all representations of ϕ by $x^2 + y^2 + z^2$ is given by*

$$(43)\qquad 24.2^{\nu} \prod_{p|2k\Delta} \chi(p).$$

Here ν denotes the number of distinct odd primes dividing $k\Delta$, and $\chi(p)$ is given for odd primes p by (41) *with $d = 1$ and in accordance with the following notations. For any prime p, set $k = p^{u_1}k_1$, $\Delta = p^{u_2 - u_1}t_1$, k_1 and t_1 prime to p. If $p > 2$, define $(m_1|p) = (k_1|p)(\phi_1|p)$ and $(m_2|p) = (m_1t_1|p)$, $\delta_1 = [(u_1+1)/2]$. If $p = 2$, then $\chi(2) = 0$, except that $\chi(2) = 1$ in the following cases:*

(44) *$u_1 + u_2$ odd; u_1 and u_2 even, $t_1 \equiv 1 \bmod 4$; u_1 even, ϕ_1 i.p., $t_1 \equiv 3 \bmod 8$; u_1 and u_2 odd, ϕ_1 p.p., $t_1 \equiv 1, 3,$ or $5 \bmod 8$.*

The number of representations in which the divisor of the representations is equal to the divisor k of ϕ is given by

$$(45)\qquad 24.2^{\nu} \prod_{p|2k\Delta} \chi_1(p),$$

where $\chi_1(p)$ is given for odd primes p by (42), *and $\chi_1(2) = 0$ except that $\chi_1(2) = 1$ in the following cases:*

$$(46)\qquad u_1 = u_2 - 1;\ u_1 = u_3 \text{ in all but the first case of } (44).$$

If $m = k^2\Delta$ and h^2 denotes the largest odd square factor common to k and Δ, then the expression in (45) *has for large m the order of size $h.0(m^{\epsilon})$, for any preassigned positive ϵ.*

Proof. It remains only to verify the values of $\chi(2)$ and $\chi_1(2)$. The form ϕ is equivalent to a form having to modulus a sufficiently high power of 2, either the residue

$$2^{u_1}m_1x_1^2 + 2^{u_2}m_2x_2^2, \text{ with } m_1m_2 \text{ odd and } 0 \leq u_1 \leq u_2,$$

if ϕ_1 is p.p., or the residue $2^{u_1}(2x_1^2 + 2x_1x_2 + 2jx_2^2)$, with j an integer, $u_1 \leq 0$, if ϕ_1 is i.p.

In the former case, the notations in (29) can be used with $p = 2$. The conditions that ϕ' must satisfy are that a_1, b_1, c_1 are integers such that either a_1 or c_1 is odd and $a_1c_1 - b_1^2 \equiv 1$ or $2 \bmod 4$, or a_1 and c_1 are even but b_1 is odd and $a_1c_1 - b_1^2 \equiv 3 \bmod 8$. Hence a_1 cannot be divisible by 4, therefore $u_1 = 2r + 1$ or $2r$.

If $u_1 = 2r + 1$, then since b_1 is integral, $q = 0$ or 2^{s-1}. If $q = 0$, then c_1 must now be odd, $u_2 = 2s$. If $q = 2^{s-1}$, then $c_1 = \frac{1}{2}m_1 + 2^{u_1-2s}m_2$ must be odd or double of an odd, hence $u_2 = 2s - 1$ and $m_1m_2 \equiv 1, 5$, or $3 \bmod 8$.

If $u_1 = 2r$, then $q = 0$, $c_1 = 2^{u_1-2s}m_2$, hence either $u_2 = 2s + 1$, or $u_2 = 2s$ and $m_1m_2 \equiv 1 \bmod 4$.

In the latter case (with ϕ_1 i.p.), ϕ' is given by

(47) $a_1 = 2^{u_1+1-2r}$, $b_1 = +2^{u_1-2r-s}(2^r - 2q)$, $c_1 = 2^{u_1+1-2r-2s}(q^2 - 2^rq + 2^{2r}j)$.

Since $4 \mid a_1$ is excluded as before, $u_1 = 2r$ or $2r - 1$.

If $u_1 = 2r - 1$, then $a_1 = 1$, $b_1 = 2^{-s}(2^{r-1} - q)$, hence $q = 2^{r-1}$ if $r - 1 < s$, $q = 0$ if $r - 1 \geq s$. If $q = 0$, then $c_1 = 2^{2r-2s}j \equiv 0 \bmod 4$, and the condition that $a_1c_1 - b_1^2 \equiv 1$ or $2 \bmod 4$ is contradicted. If $q = 2^{r-1}$, then $c_1 = 2^{2r-2-2s}(4j - 1)$, which is not integral since $r - 1 < s$, a contradiction.

There remains $u_1 = 2r$, $a_1 = 2$. If $s = 0$, then $q = 0$, $b_1 = 2^r$, $c_1 = 2^{2r+1}j$, hence $r = 0$ and j must be odd. If $s = 1$, then $r \geq 1$ since b_1 is integral, $q = 0$ since c_1 is integral, hence $r = 1$ and j must be odd since ϕ' can only be i.p. Let $s \geq 2$. Then $r \geq 2$ and q is even since b_1 and c_1 are integral. If $r \geq s$, we may set $q = 2^{s-1}k$ ($k = 0$ or 1), have $c_1 = 2^{1-2s}(2^{2s-2}k^2 - 2^{r+s-1}k + 2^{2r}j)$, k even, $k = 0$, $r = s$ and $j = 1$. If $r < s$, we may set $q = 2^{r-1} + 2^{s-1}k$ ($k = 0$ or 1), $c_1 = \frac{1}{2}\{k^2 + (4j - 1)2^{2r-2s}\}$ which cannot be an integer. Thus there are no solutions in the case with ϕ_1 i.p. unless u_1 is even and j is odd, and then q, r, and s are uniquely determined.

From this, (44) readily follows, and then by taking $r + s = u_1$, also (46).

In Linnik's application to proving that (under certain conditions) a large number is represented by each class of a ternary genus, it was assumed that m is prime to the determinant d of the genus. The determinant of the binary quadratic form $\phi = k\phi_1$, which is to be represented by a ternary form of determinant d^2 happens to be of the form $b_1 = m - q_1k$, where q_1 is an integer and k is the divisor of ϕ. Hence the assumption that m is prime to d implies that k is prime to d. To fill the gap in Linnik's proof it therefore suffices to prove the following theorem.

THEOREM 5. *Consider a representative set of forms $f_1, \ldots, f_s$ with integral matrices of a given non-zero determinant d, and an integral binary quadratic form $\phi = k\phi_1$ (ϕ_1 p.p. or i.p.) of determinant $b_1 = k^2\Delta$, where k is prime to d. Let h^2 denote the largest square factor common to k and Δ. Let ρ denote the number of sets of representations of ϕ by $f_1, \ldots, f_s$ such that the divisor of the representations is k. Then for any positive ϵ, there exists a constant q, depending on ϵ and d, but independent of b_1 and ϕ, such that*

$$\rho < qh(b_1)^{\epsilon}. \tag{48}$$

Proof. The condition of primitive representation is, as in (26),

$$b'k_1^2 - 2t'k_1k_2 + a'k_2^2 \equiv -d \pmod{b_1}. \tag{49}$$

Hence the divisor k of $\phi = a'x^2 + 2t'xy + b'y^2$ must divide d. If k is prime to d this implies that $k = 1$. Accordingly, the representations of divisor k of the form $\phi = k\phi_1$ by ternaries of determinant d are associated with primitive

representations of forms which are properly or improperly primitive, and which represent $-d$ modulo Δ, where $\Delta = |\phi_1|$. The theorem is therefore a consequence of the following three lemmas.

LEMMA 7. *Let* $b_1 = \prod_{i=1}^{r} p_i^{\beta_i}$ *express* b_1 *as a product of powers of distinct primes. Then the number of divisors of* b_1, *namely* $\prod(\beta_i + 1)$, *is* $0\ (b_1^{\epsilon})$ *for every positive* ϵ. *Hence,* $2^{\nu} = 0(b_1^{\epsilon})$ *and* $5^{\nu} = 0(b_1^{\epsilon})$.

Proof. See [14].

LEMMA 8. *If* a', t', *and* b' *are relative prime, the number of solutions* K *modulo* B_1 *of* (49) *does not exceed* $4d.2^{\nu}$, *where* ν *denotes the number of distinct odd primes dividing* b_1.

Proof. If $[a', 2t', b']$ is i.p., then $b_1 = a'b' - t'^2$ is odd, and the prime 2 does not affect the result. Hence for any prime p dividing b_1, ϕ can be given the residue $m_1x_1^2 + p^{u_2}m_2x_2^2 \pmod{p^s}$, where m_1 and m_2 are prime to p and p^s is the precise power of p dividing b_1. Then (49) becomes $p^s m_2 k_1^2 + m_1 k_2^2 \equiv -d \pmod{p^s}$, for each p^s. Hence k_1 has p^s values modulo p^s, or b_1 values modulo b_1, and this is cancelled by the factor b_1 due to Lemma 5. Also k_2 can have at most $4p^{\beta}$ residues modulo p^s if $p^{2\beta} | d$ and $p^{2\beta+2}$ does not divide d, and $p^{2\beta} | p^s$; and at most $p^{[\frac{1}{2}s]}$ residues modulo p^s if $p^s | d$.

LEMMA 9. *The number of systems of values* r, s, q *for which the form* ϕ' *in* (29) *is primitive modulo* p, *but such that* $r + s = u_1$, *does not exceed* $5(u_1 + 2)p^{\sigma}$, *where* p^{σ} *denotes the precise power of* p *dividing* h (*cf. last statement of Theorem* 4). *This holds true for* $p = 2$, *with* ϕ' *given either by* (29) *or* (47).

Proof. We follow the steps in § 8, dropping the condition that ϕ' represent $-d$ mod p, and noticing whether the statements are valid also for $p = 2$. The number of systems r, s, q satisfying $r + s = u_1$ and (30), or (31), is at most 1. From (32) are derived if p is odd less than $2(u_1 + 1)$ values r, s, q, indeed $2\delta_1$ values if $u_1 = u_2$, none if $u_1 < u_2$. If $p = 2$, (32) gives at most four values q_1 mod p^{s-t}, hence at most $2(u_1 + 1)$ values r, s, q. We have (33) (a) as before, with at most $p^{\sigma} - 1$ systems r, s, q if $\frac{1}{2}u_2 \leq u_1 < u_2$, zero otherwise. In (33) (b), if $2s = u_2$, we replace θ by $p - 1$ (taking q_1 arbitrary), and thus obtain at most $(p-1)p^{\sigma-1}$ systems, r, s, q. If $2s > u_2$, the number of systems obtained is at most twice that obtained earlier, hence at most $2(u_1 + 1)(p-1)p^{\sigma-1}$. In (33) (c) we may replace η_1 by 1 and have at most $p^{\frac{1}{2}u_1} - 1$ if $u_1 < \frac{1}{2}u_2$, $p^{\nu} - 1$ if $\frac{1}{2}u_2 \leq u_1 < u_2$, —in both cases $p^{\sigma} - 1$. The sum total does not exceed $2(u_1 + 3)\, p^{\sigma}$.

The factor for $p = 2$ due to case (47) remains to be considered. The possibility a_1 and b_1 even, c_1 odd, with $r + s = u_1$, is easily seen to be contradictory. If a_1 is odd, then $r = \frac{1}{2}(u_1 + 1)$, $s = u_1 - r$, and since b_1 is an integer, q has 2 residues modulo 2^s. Finally, consider a_1 even, b_1 odd. Since $r + s = u_1$, $1 - 2^{t-r}q$ is odd. There are $1 + [u_1/2]$ values q, r, s with $q = 0$. If $q \neq 0$, we may set $q = 2^t q_1$, must have $s > t \geq r$, while

$$c_1 = \{(2^{t-r+1}q - 1)^2 + 4j - 1\}/2^{s-r+1}.$$

Thus $2^{t-r+1}q_1 - 1$ has at most two residues mod 2^{s-r}, and hence q has at most

four residues mod 2^s. Thus there are at most $4(u_1+1)$ complexes q, r, s. The total due to (47) does not exceed $5(u_1+2)$.

9. Adjoint representations. Gauss, Smith, and Minkowski used a somewhat different algorithm from that which we have described in the preceding. They made use of the case $k = 1$ or $n - 1$ of a correspondence (which will here be simplified and generalized) between the primitive representations of a form ϕ in k variables by a form f in n variables, and the primitive representations of a certain related form ψ in $n - k$ variables by the adjoint of f.

Certain aspects of their treatments are superfluous, as for example the insistence upon dealing with integral forms, and this fact hides the essential simplicity of the correspondence. Indeed, the forms ϕ and ψ, f and adj f, are also in a certain measure superfluous, and the correspondence is basically one between *adjoint representations* described as follows.

Consider $(S_1\ S_2)^{\mathsf{T}} = (T_1\ T_2)^{-1}$, where $(T_1\ T_2)$ is unimodular. If T_2 is replaced by any complement $T_1H + T_2U$ of T, then T^{-1} is replaced by

$$(50)\qquad \left((T_1\ T_2)\begin{bmatrix} I_1 & H \\ 0 & U \end{bmatrix}\right)^{-1} = \begin{bmatrix} I_1 & -HU^{-1} \\ 0 & U^{-1} \end{bmatrix}\begin{bmatrix} S^{\mathsf{T}}{}_1 \\ S^{\mathsf{T}}{}_2 \end{bmatrix} = \begin{bmatrix} S^{\mathsf{T}}{}_1 - HU^{-1}S^{\mathsf{T}}{}_2 \\ U^{-1}S^{\mathsf{T}}{}_2 \end{bmatrix}$$

and hence S_2 is replaced by $S_2(U^{\mathsf{T}})^{-1}$. Similarly, if S_1 is replaced by any left complement $S_1V + S_2J$ (V unimodular, J integral) of S_2, then T_1 is replaced by $T_1(V^{\mathsf{T}})^{-1}$. Thus the two *aggregates* of representations T_1V and S_2U, where $V^{(k,k)}$ and $U^{(n-k,n-k)}$ are arbitrary unimodular matrices, are *adjoint* to one another in the following sense. For any U and V, T_1V has a right complement T_2, and S_2U has a left complement S_1 such that $(S_1\ S_2U)^{-1} = (T_1V\ T_2)^{\mathsf{T}}$. Only the matrices T_1V and S_2U arise from one another in this manner.

Consider now (10) and (11). If T_2 is replaced by any complement $T_1H + T_2U$ of T_1, D_2 is replaced by the equivalent matrix $U^{-1}D_2(U^{\mathsf{T}})^{-1}$. This coincides with D_2 if and only if U^{T} is a unimodular automorph of D_2. Similarly, if S_1 is replaced by other complements, T_1 is replaced by $T_1(V^{\mathsf{T}})^{-1}$, and this is a representation of B_1 by A if and only if V^{T} is a unimodular automorph of B_1.

It follows that there is associated, with the *ensemble* of primitive representations (T_1V) of B_1 by A (where V runs through all unimodular automorphs of B_1), in a unique manner an ensemble of primitive representations (S_2U) of D_2 by adj A (where U ranges over the unimodular automorphs of D_2); and conversely.

Representations of non-equivalent matrices B_1 and B'_1 by A cannot be associated with the same ensemble of primitive representations of D_2 by C, since the replacement of S_1 by other complements of S_2U replaces B_1 by an equivalent matrix.

If B_1 is replaced by an equivalent matrix $Z^{\mathsf{T}}B_1Z$ (Z unimodular), and T_1 by T_1Z, the matrices S_2U are unaltered. Thus, corresponding primitive representations of $Z^{\mathsf{T}}B_1Z$ by A are associated with the same representations of D_2 by C as are those of B_1 itself.

Since at least one minor determinant of order k in T_1 is not zero, $T_1V = T_1V'$ implies $V = V'$. Hence as V ranges over the unimodular automorphs of B_1, the matrices T_1V are distinct; and similarly for S_2U.

If $k = n - 1$, and A and B_1 are integral, then D_2 is an integer d_2, and B_1 is an integral $(n-1)$-ary matrix of determinant d_2. Hence all the primitive representations of d_2 by C can be obtained by choosing one matrix B_1 from each of the finite number of classes of determinant d_2, and constructing the primitive representations of T_1 of each such B_1 by A. The number of ensembles of primitive representations (T_1V) will now be exactly equal to the number of primitive representations of d_2 by C, since a unary D_2 has only one unimodular automorph.

Gauss, Smith, and Minkowski made use of this correspondence to reduce the problem of representing numbers to that of representing $(n-1)$-ary forms.

It should be observed, finally, that in general, for a given A, a correspondence can be set up between ensembles of primitive representations of a set of non-equivalent matrices $B_1^{(i)} (i = 1, \ldots, h_1)$ by A, and a set of non-equivalent matrices $D_2^{(j)}$ $(j = 1, \ldots, h_2)$ by adj A. As noted in (14), the determinants satisfy $d_2 = b_1 a^{n-k-1}$; and the matrices D_2 satisfy adj $G = b_1^{n-k-2} D_2$, with B_1 one of the $B_1^{(i)}$, and $b_1^{-1}G$ the matrix obtained by completing squares with reference to B_1 in B. The corresponding sets of matrices can be determined precisely in particular cases.

Thus, for example, if $n = 3$, $A = C = I$, $k = 1$, and b_1 is a positive integer, the matrices $D_2^{(j)}$ are representatives of the s classes of the genus described in § 6, and each such matrix has $24.2^r/u$ ensembles of primitive representations by adj A, if we assume that $b_1 \not\equiv 0, 4, 7 \bmod 8$. Hence, as before, the number of primitive representations of b_1 by $x^2 + y^2 + z^2$ is equal to $s\ 24\ 2^r/u$. Thus, the representations of $2x_1^2 + 2x_1x_2 + 2x_2^2$ as $(a_1x_1 + b_1x_2)^2 + (a_2x_1 + b_2x_2)^2 + (a_3x_1 + b_3x_2)^2$ will be found by trial to be 48 in number, and since this binary form has six unimodular automorphs they comprehend 8 ensembles,—corresponding to the 8 representations of 3 as a sum of three squares. Similarly, it may be verified that $2x_1^2 + 2x_1x_2 + 2x_2^2$ has 48 representations by $x^2 + y^2 + z^2 + 2w^2$, comprehending $48/6 = 8$ ensembles; and that these are associated with 16 representations of $x_1^2 + 6x_2^2$ by $2x^2 + 2y^2 + 2z^2 + w^2$, hence $16/2 = 8$ ensembles.

10. The alternative algorithm based on the adjoint form. The method used by Gauss, Smith, and Minkowski differed from ours in one further respect. What they did (in the case $k = n - 1$) was, essentially, to construct the adjoint matrix D in (11) rather than B.

If T_2 is replaced by any complement $T_1H + T_2U$, D is transformed by

$$\left(\begin{bmatrix} I_1 & H \\ 0 & U \end{bmatrix}^{-1}\right)^{\mathrm{T}} = \begin{bmatrix} I_1 & 0 \\ -(U^{\mathrm{T}})^{-1}H^{\mathrm{T}} & U^{\mathrm{T}-1} \end{bmatrix},$$

and hence D_2 is replaced by $U^{-1}D_2(U^{\mathrm{T}})^{-1}$ and L by $U^{-1}L - U^{-1}D_2(U^{\mathrm{T}})^{-1}H^{\mathrm{T}}$. If we choose a particular matrix D_2 in its class, $(U^{\mathrm{T}})^{-1}$ (and also U^{T}) is re-

stricted to be a unimodular automorph of D_2, and L is replaced by $U^{-1}L - D_2H^T$. Thus the set of primitive representations (WT_1) of B_1 by A is associated with a matrix D_2 and a *complex of solutions* L of the congruence

$$L^T(\text{adj } D_2)L \equiv -a^{n-k} \text{ adj } B_1 \pmod{d_2}. \tag{51}$$

Here, two matrices L and L' are defined to be in the same complex of solutions of (51) if there exists a unimodular automorph U^T of D_2 such that $U^{-1}L$ and L' are in the same left-sided residue class modulo D_2. An equation similar to (25) can be formulated, it being necessary to confine attention to solutions L of (51) such that if D_1 is defined by

$$L^T(\text{adj } D_2)L + a^{n-k} \text{ adj } B_1 = d_2D_1, \tag{52}$$

then the matrix D (formed as in the last member of (11)) is equivalent to one of adj $A', \ldots,$ adj $A^{(\lambda)}$.

The case $k = n - 1$ is particularly simple. Then $D_2 = d_2 = b_1$, adj $D_2 = 1$, and the only automorph U^T of D_2 is 1. Congruence (51) becomes

$$L^TL \equiv -a \text{ adj } B_1 \pmod{b_1}, \tag{53}$$

and two matrices L and L' are in the same complex if and only if $L \equiv L' \bmod b_1$. Accordingly, there is a 1-1 correspondence between the solutions $L \bmod b_1$ of (51), such that the resulting matrices D are equivalent to one of the adj $A^{(i)}$, and the sets (WT_1) of primitive representations of B_1 by the system of matrices $A^{(i)}$.

References

[1] U. V. Linnik, "On the Representation of Large Numbers by Positive Ternary Quadratic Forms," *Bull. Acad. Sci. USSR, math. ser.*, vol. 4 (1940), 363-402.
[2] H. D. Kloosterman, *Acta Math.*, vol. 49 (1926), 407-464.
[3] W. Tartakowsky, *Bull. Acad. Sci. Leningrad* (7) 2 (1929), 111-122 and 165-196.
[4] G. Pall, *Amer. J. Math.*, vol. 68 (1946), 47-58; A. E. Ross and G. Pall, *Amer. J. Math.*, vol. 68 (1946), 59-65.
[5] B. W. Jones and G. Pall, *Acta Math.*, vol. 70 (1939), 165-191.
[6] J. W. L. Glaisher, *Quart. J. Math.*, vol. 20 (1885), 94.
[7] B. A. Venkov, *Elementary Theory of Numbers* (Russian), 1937.
[8] G. Pall, *Amer. J. Math.*, vol. 64 (1942), 503-513.
[9] U. V. Linnik, *Rec. Math.* [*Mat. Sbornik*] N.S., vol. 12 (54), (1943), 218-224.
[10] C. L. Siegel, *Ann. of Math.*, vol. 36 (1935), 527-606.
[11] C. Hermite, *J. für Mathematik*, vol. 47 (1850), 192.
[12] H. J. S. Smith, *Collected Mathematical Papers* (Oxford, 1894).
[13] C. F. Gauss, *Disquisitiones Arithmeticae*, 1801, Arts. 278-283.
[14] G. H. Hardy and E. M. Wright, *The Theory of Numbers* (Clarendon Press, 1938), p. 259.
[15] A. Schild, *Can. J. Math.*, vol. 1 (1949), 47.

Illinois Institute of Technology
Chicago

GRAPHS OF DEGREE THREE WITH A GIVEN ABSTRACT GROUP

ROBERT FRUCHT

1. Introduction. In his well-known book on graphs [1] König proposed the following problem: "When can a given abstract group be represented as the group of the automorphisms of a (finite) graph, and if possible how can the graph be constructed?"

To understand this problem well let us begin with the precise definition of a graph and its group (of automorphisms).

A (finite) graph is a finite set of points or vertices $A, B, C, \ldots$, and edges or arcs which join certain pairs of these vertices; i.e. for each pair of distinct vertices P, Q, there is given an adjacency number $I_{P,Q} = I_{Q,P}$ such that

$$I_{P,Q} = I_{Q,P} = \begin{cases} 0, \text{ if the graph does not contain an edge } PQ \\ n, \text{ if the graph contains } n \text{ edges joining } P \text{ with } Q. \end{cases}$$

To exclude "isolated" vertices König postulates also that each vertex is the endpoint of at least one edge; i.e. for each vertex A of the graph there is at least another vertex Q such that $I_{A,Q} \neq 0$. (We will not consider the more general graphs—called by König "Graphen im weiteren Sinne"—where an edge may have two coincident endpoints, i.e. where also adjacency numbers $I_{P,P}$ exist, some of them having the value 1.)

The group of automorphisms of a graph, or shortly the group of a graph, may then be defined as the set of all the mappings of the graph into itself, i.e. of all the permutations of the vertices and edges which preserve incidence-relations.

An equivalent, but more algebraic definition of the group of a finite graph may be given for the more restricted class of the graphs having no pairs of edges forming a closed circuit; in such graphs any two vertices are either adjacent or "neighbours"—and in this case there is just one edge joining them—or not adjacent. For this more restricted class of graphs *where the adjacency numbers only can be* 0 *or* 1, the following definition of their group may be given:

Let to every vertex P_i of the graph correspond a variable x_i; then the graph will be fully described by the *quadratic form* $\sum_{i<k} I_{P_i,P_k} x_i x_k$, and the group of the graph will be nothing else than the group of all the permutations of the x_i which leave that quadratic form unaltered.

Returning now to König's problem, it might be stated more concisely in the following terms: Given any finite group $\mathfrak{H}$ find a graph G whose group is simply isomorphic to $\mathfrak{H}$.

Received September 13, 1948.

It has been shown by the author [2] that this problem has always a solution by giving for any group $\mathfrak{H}$ of order $h > 1$ the construction of a graph with $2h^3 - h^2$ vertices; this number may be reduced to $h(n+1)(2n+1)$, when one knows n elements of the group $\mathfrak{H}$ which generate the whole group. For the case $h = 1$ the author gave in the same paper an example of a graph with 7 vertices; later on Kagno [3] succeeded in finding a graph with only 6 vertices which has no non-identical group.

It is obvious that for some special groups there are also graphs with fewer vertices than $h(n+1)(2n+1)$; e.g. for the symmetric group $\mathfrak{S}_N$ with $h = N!$ and $n = 2$, we have a graph with only N vertices, namely the "complete N-point" in which any two distinct vertices are joined by an edge.

But it turns out that also in general the number of vertices needed by the author in his former paper for the construction of a graph with given abstract group is rather excessive, and the main object of this paper is to give a new solution of König's problem by a graph with fewer vertices and fulfilling also the additional condition of being "regular of degree 3" or "cubical."

As to the last condition it must be remembered that *degree* of a vertex A is called the number of edges having one of their endpoints in A, i.e. the sum $\sum_P I_{A,P}$, where P runs through all the vertices of the graph; and when all the vertices of a graph are of the same degree r, König calls the graph "*regular of degree r*." Recently the graphs which are regular of degree 3 have been called "*cubical*" by Tutte [4], and we will use this shorter name too. The outstanding interest these cubical graphs deserve in the theory of graphs seemed to us to justify a study of König's problem for this special class of graphs, and the rather surprising result (Theorem 4.1) was that in spite of this new condition of regularity of degree 3 there is always a cubical graph with only $2h(n+2)$ vertices whose group is simply isomorphic to a given abstract group $\mathfrak{H}$ of order $h > 2$ and generated by n of its elements; for $h = 1$ or 2 there are cubical graphs with 12 or 10 vertices respectively (Theorems 2.3 and 2.4).

Also in the case of cubical graphs it cannot be claimed that $2h(n+2)$ vertices are always necessary, since for some special groups cubical graphs with fewer vertices are known; e.g. the "complete 4-point" for the group $\mathfrak{S}_4$ ($h = 24$, $n = 2$), Petersen's graph [5] with 10 vertices for $\mathfrak{S}_5$ ($h = 120$, $n = 2$), Kagno's graph [6] H_{17} with 6 vertices for the dihedral group of order 12, etc.

The same general principle underlying the construction of a cubical graph may also be slightly modified to give a new solution of König's problem in its primitive form (i.e. without postulating that the graph be cubical); instead of $h(n+1)(2n+1)$ the number of vertices needed for the construction will now (Theorems 3.2 and 4.2) be: $2hn$ for non-cyclic groups, and $3h$ for cyclic groups ($n = 1$) of order $h > 3$; if $h = 3$ it seems that a tenth vertex is indispensable.

Finally it must be emphasized that König's problem has been interpreted here in the sense that only *simple isomorphism* between the given group and that of the graph is required. If the given group is a permutation group $\mathfrak{P}_N$

on N symbols, there would be also the problem of finding a graph with the same number N of vertices, and whose group is *identical* with $\mathfrak{P}_N$. However this more difficult problem has not always solutions; e.g. Kagno showed [6] that there are no graphs when $\mathfrak{P}_N$ is a cyclic or an alternating group ($N > 3$), and gave for $N \leq 6$ a complete list of all the cases where a solution exists. It seems that the general case ($N \geq 7$) of this problem has not yet been treated.

2. Types; cubical graphs with groups of order 1 and 2. In this section we are only dealing with cubical graphs having no adjacency number > 1.

We begin with the introduction of the notion of the "type" (κ, λ, μ) of a vertex; this notion will prove to be useful in the investigation of the group of a cubical graph.

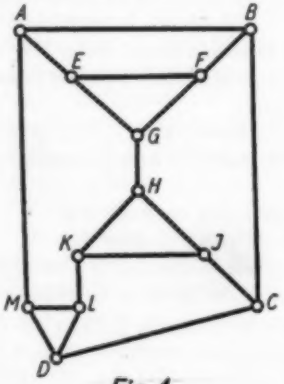

Fig. 1

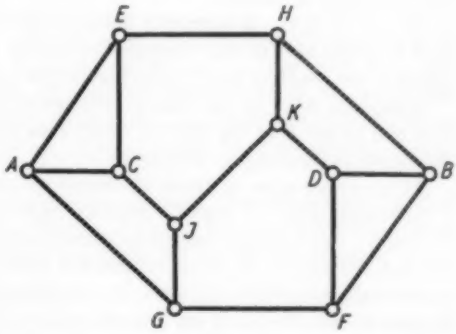

Fig. 2

In a cubical graph without adjacency numbers > 1 any vertex P has 3 distinct neighbours, say P_1, P_2, P_3. It may happen that there is no closed polygon or ν-circuit that contains the two edges PP_1 and PP_2; then let $\kappa = \infty$. (Here a closed polygon or ν-circuit is defined as a set of ν edges, A_1A_2, A_2A_3, $A_3A_4, \ldots, A_{\nu-1}A_\nu, A_\nu A_1$, such that no two of the ν vertices $A_1, A_2, A_3, \ldots, A_\nu$ coincide.) Otherwise there will be one or more closed polygons containing the edges PP_1 and PP_2; then let κ be the least value of ν for which such a ν-circuit exists. In an analogous manner define λ for the two edges PP_1 and PP_3, and μ for the two edges PP_2 and PP_3. Of course, since the enumeration of the 3 neighbours of P was arbitrary, we always may suppose that $\kappa \leq \lambda \leq \mu$. Then the number-triple (κ, λ, μ) will be called the *type* of the vertex P.

As an example consider the cubical graph of Figure 1 which can be drawn in the plane; it has 12 vertices (and hence 18 edges). Let us begin with determining the type of A. This vertex is endpoint of the edges AB, AE, and AM. The pair AB, AE occurs in the 4-circuit $AEFBA$ (but in no ν-circuit with $\nu<4$); the pair AE, AM occurs in the 7-circuits $AEFBCDMA$ and $AEGHKLMA$, but in no closed polygon with fewer than 7 vertices; finally the pair

AB, AM is contained in the 5-circuit $ABCDMA$, but in no ν-circuit with $\nu < 5$. Hence the type of the vertex A is (4, 5, 7).

In an analogous manner the following table of types for each vertex of the graph of Figure 1 was obtained:

A . . . . . (4, 5, 7)
B . . . . . (4, 5, 6)
C . . . . . (5, 5, 6)
D . . . . . (3, 5, 5)
E, F . . . . . (3, 4, 5)
G, H . . . . . (3, 6, 7)
J, K, L, M . . . . . (3, 5, 6)

The usefulness of this notion of type results from the following two theorems (whose proof is obvious):

THEOREM 2.1. *A necessary (but not sufficient) condition that a vertex P of a cubical graph may be taken into another vertex Q by a permutation belonging to the group of the graph is that P and Q are of the same type.*

THEOREM 2.2. *If for some 3 numbers $\kappa \leq \lambda \leq \mu$ there is in a cubical graph just one vertex P of the type (κ, λ, μ), then P is left fixed by each permutation belonging to the group of the graph.*

As an application of these theorems we are now going to prove the

THEOREM 2.3. *The graph given by Figure 1 has a group of order 1.*

Proof. Let τ be any mapping of the graph into itself. According to Theorem 2.2 the vertices A, B, C, and D are left fixed by τ. The Theorem 2.1 does not exclude the possibility that the vertex E could be changed into F by τ, but it is easy to see that such an interchange of E and F is not possible, as E is a neighbour of the invariant vertex A, but F is not. Hence also E is left fixed by τ, and F too. This last vertex has the neighbours B, E, and G, but since B and E are left fixed by τ, also G is. Of the same type as G is only the vertex H, but as we already know that G remains invariant, also H must be left fixed by τ. As to the 4 vertices of type (3, 5, 6) it is easy to see that J is left unchanged by τ as the only common neighbour of C and H; K as the only common neighbour of H and J; L as the only common neighbour of D and K; finally M remains fixed, because all the other vertices of the graph are left unchanged by τ. Thus τ does not change any vertex, and as τ was any mapping of the graph into itself, it has been proved that the group of this graph consists only of the identity.

As another example of the use of types let us consider the cubical graph of Figure 2; it has 10 vertices (and 15 edges). We will now prove the

THEOREM 2.4. *The graph given by Figure 2 has a group of order 2.*

Proof. Here we have the following types:

A, B, C, D . . . . . (3, 4, 5)
E, F . . . . . (3, 5, 6)
G, H . . . . . (4, 5, 6)
J, K . . . . . (4, 5, 5)

It is obvious that this graph admits (beside the identity) the following permutation of order 2:

$$\sigma = \begin{pmatrix} A\ B\ C\ D\ E\ F\ G\ H\ J\ K \\ B\ A\ D\ C\ F\ E\ H\ G\ K\ J \end{pmatrix}.$$

Let τ be any mapping of the graph into itself; we must show that τ is either σ or the identity. Let us distinguish two cases:

Case 1: τ leaves the vertex G unchanged. Of the same type as G is only the vertex H which in this case must be left fixed too. The 3 neighbours of the fixed-point G, namely A, F, J, are of distinct types; hence they cannot be permuted among themselves by τ, but must be left fixed too. The same consideration for the neighbours of H shows that the same is true for B, E, K. Finally C must be left fixed by τ, as it is the only common neighbour of the fixed-points A and E; and D remains fixed, as it has "no other choice." Hence in this case τ is the identity.

Case 2: τ interchanges G and H. (According to Theorem 2.1 there are no other possibilities.) Then consider the "product" $\tau\sigma$, i.e. the mapping τ followed by the mapping σ defined above. Since τ takes G into H, and σ changes H into G, the product $\tau\sigma$ leaves G unchanged. Applying the considerations of case 1 to $\tau\sigma$ (instead of τ) we see that $\tau\sigma$ must be the identity; hence $\tau = \sigma^{-1} = \sigma$.

It would be easy to see that another graph with 12 vertices and group of order 1 (but different from that of Figure 1) might be obtained from that of Figure 2 by joining the mid-points of the edges AG and CJ by an edge.

3. Cubical graphs with cyclic groups.

THEOREM 3.1. *If $\mathfrak{H}$ is the cyclic group of order $h > 2$, there is a cubical graph with $6h$ vertices whose group is simply isomorphic to $\mathfrak{H}$.* (For the case $h = 2$ see Theorem 2.4).

Proof. Let $h > 2$. The quadratic form in $6h$ variables $a_i, b_i, c_i, d_i, e_i, f_i$ $(i = 1, 2, \ldots, h)$:

$$\sum_{i=1}^{h} (a_ib_i + a_ie_i + a_if_i + b_ic_i + c_id_i + c_if_i + e_if_i) + \sum_{j=1}^{h-1} (b_je_{j+1} + d_jd_{j+1}) + b_he_1 + d_1d_h$$

defines (see introduction) a cubical graph with $6h$ vertices (which will be indicated by the same letters a_i, b_i, etc.); it has to be shown that its group is simply isomorphic to the cyclic group of order h.

In Figure 3 this graph is given for the case $h = 5$; in this case the types of the vertices are (always for $i = 1, 2, 3, 4, 5$):

a_i and f_i . . . . . (3, 4, 5)
b_i . . . . . (4, 7, 9)
c_i . . . . . (4, 7, 7)
d_i . . . . . (5, 7, 7)
e_i . . . . . (3, 7, 8).

In the general case of any h whatsoever the types would be the same except that of the vertices d_i which would be $(h, 7, 7)$ or $(7, 7, h)$ if $h \leq 11$, and $(7, 7, 11)$, if $h > 11$.

It is obvious that any cyclic permutation of all the suffices does not change the graph; we must therefore only show that any mapping τ of the graph into itself is either the identity or some cyclic permutation of all the suffices, i.e. some power of the permutation ω which changes each a_i into a_{i+1} (except a_h which is taken into a_1), each b_i into b_{i+1} (except b_h which is changed into b_1), etc.

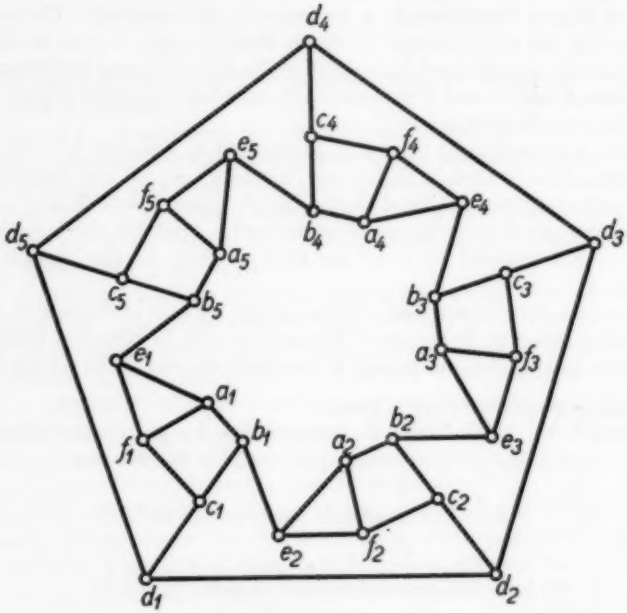

Fig. 3

In the proof we may distinguish two cases:

Case 1: τ leaves b_1 unchanged. Since the neighbours of b_1, namely a_1, c_1, e_2, are of distinct types, they cannot be permuted among themselves by τ, and are left fixed. The same argument holds for the neighbours of a_1, leading to the conclusion that also e_1 and f_1 remain unaltered. Hence, since two of the 3 neighbours of the fixed-point c_1, viz. b_1 and f_1, do not change, also the third, d_1, must be left unchanged by τ; and the same is true for b_h, the third neighbour of e_1 (beside a_1 and f_1). Now the same chain of considerations may be repeated for the vertices with subscript h, leading to the conclusion that they remain all unchanged by τ, and b_{h-1} too. Then the same considerations may be repeated

for the vertices with subscript $h-1$, etc., until the final conclusion is reached that no vertex is changed by τ; thus τ is the identity in this case.

Case 2: If τ changes b_1 into some other vertex, according to Theorem 2.1 (and the list of types given above) that other vertex must be a b_i too ($i = 2, 3, 4, \ldots, h$), say b_j. But there is also the mapping ω^{j-1} which takes b_1 into b_j (as ω changes b_i into b_{i+1}); hence the product $\tau(\omega^{j-1})^{-1}$ leaves b_1 unchanged and is therefore the identity (see Case 1); that means that $\tau = \omega^{j-1}$.

Having thus proved the Theorem 3.1, it may be remarked that a graph with fewer vertices than $6h$ can be found, when we remove the restriction that the graph is to be cubical:

THEOREM 3.2. *If $\mathfrak{H}$ is the cyclic group of order $h > 3$, there is a graph with $3h$ vertices whose group is simply isomorphic to $\mathfrak{H}$.*

If $h = 2$, there is of course the graph consisting only of two vertices joined by one edge. The case $h = 3$ seems to be exceptional, as I did not succeed in finding a graph with 9 vertices (or fewer); one with 10 vertices is given by Figure 4.

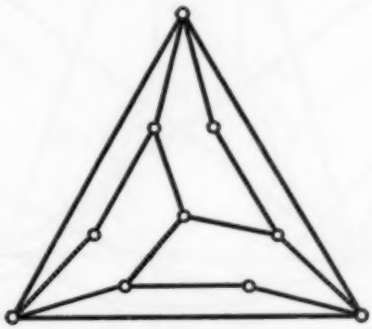

Fig. 4

Proof of Theorem 3.2. Let x_i, y_i, z_i ($i = 1, 2, \ldots, h$) be $3h$ variables, and consider the graph defined by the quadratic form:

$$\sum_{i=1}^{h}(x_iy_i+y_iz_i)+\sum_{j=1}^{h-1}(x_jx_{j+1}+z_jx_{j+1})+x_1x_h+x_1z_h+\sum_{k<l}z_kz_l;$$

for $h = 5$ see Figure 5. In this graph each vertex x_i is of degree 4, each vertex y_i is of degree 2, and each vertex z_i is of degree $h+1$. The proof that the group of this graph is simply isomorphic to the cyclic group of order h (if $h > 3$) is very easy.

Case 1: If any mapping τ of the graph into itself leaves x_1 unchanged, it must leave fixed also y_1, the only neighbour of x_1 having degree 2; hence τ leaves unchanged also z_1, the other neighbour of y_1. Now z_1 has only one neighbour of degree 4, namely x_2, which must be left fixed too, etc. Going on in this way it is easily seen that τ is in this case the identity.

Case 2: If τ changes x_1 into another x_j (and there are no other possibilities if $h > 3$), then the product $\tau(\gamma^{j-1})^{-1}$ will be the identity, when γ is the substitution changing each x_i into x_{i+1}, each y_i into y_{i+1}, each z_i into z_{i+1} (being understood that for $i = h$ the subscript $h + 1$ is to be replaced by 1).

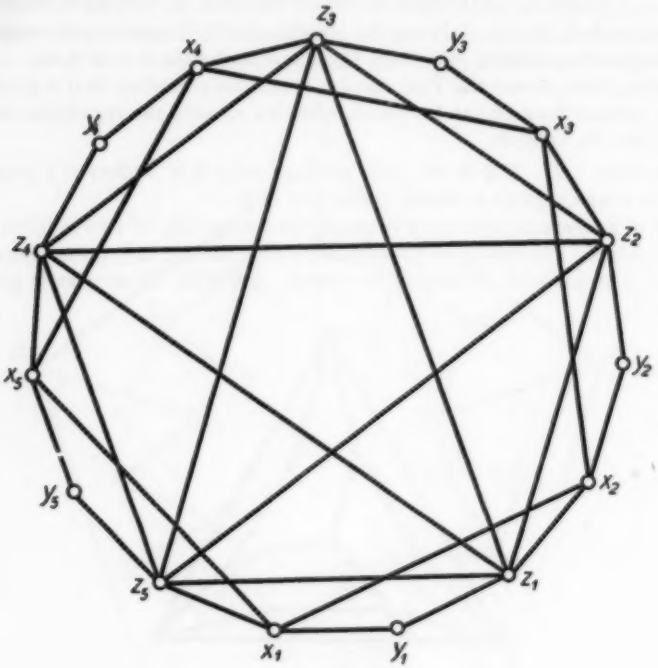

Fig. 5

As a final remark on Theorem 3.2 we wish to emphasize that there may be graphs with still fewer vertices than $3h$ (at least for certain values of $h > 3$). This is readily verified when the order of the cyclic group is not a prime nor a prime power. E.g. let $h = p^\alpha q^\beta$ (p and q being distinct primes); since $\mathfrak{H}$, the cyclic group of order h, is then the direct product of a cyclic group of order p^α and another cyclic group of order q^β, and since these groups have (according to Theorem 3.2) graphs with $3p^\alpha$ and $3q^\beta$ vertices respectively, these two graphs together form a (not connected) graph with only $3(p^\alpha + q^\beta)$ instead of $3h = 3p^\alpha q^\beta$ vertices and belonging to the same group $\mathfrak{H}$. (By adding $9p^\alpha q^\beta$ edges between each vertex of the one component and each of the other, also a connected graph with the same number of vertices and the same abstract group could be obtained.)

4. Cubical graphs with non-cyclic groups.

THEOREM 4.1. *If $\mathfrak{H}$ is any finite group of order $h \geqq 3$ which may be generated by n of its elements, then it is always possible to find a cubical graph with $2(n+2)h$ vertices that has a group simply isomorphic to $\mathfrak{H}$.*

Proof. If $n = 1$, the group is cyclic, and the Theorem 4.1 is only a restatement of Theorem 3.1.

If $n > 1$, let the elements of the given abstract group $\mathfrak{H}$ be enumerated as follows: let H_h be the unit of the group, and $H_1, H_2, H_3, \ldots, H_n$ the n elements generating the group; $H_{n+1}, H_{n+2}, \ldots, H_{h-1}$ will be the other elements of $\mathfrak{H}$.

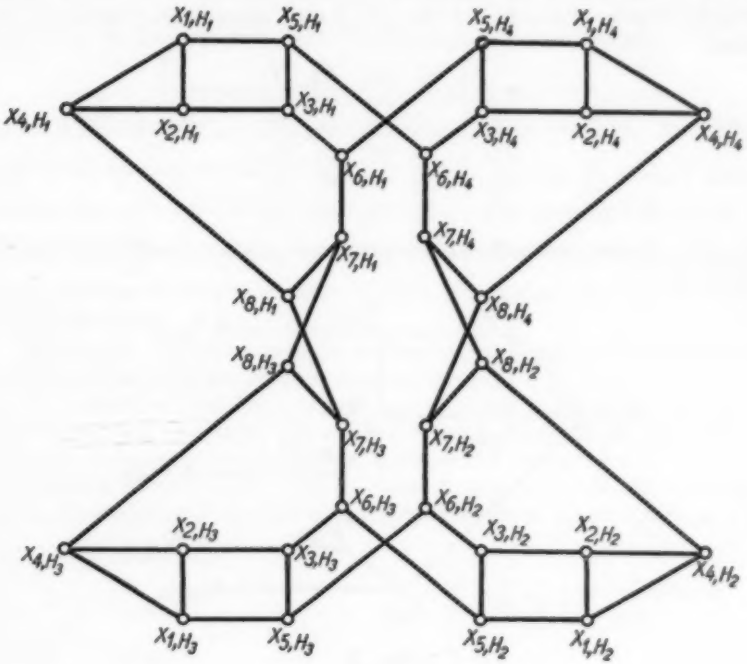

Fig. 6

To obtain a cubical graph with a group simply isomorphic to $\mathfrak{H}$ let us introduce $(2n+4)h$ variables x_{i,H_k} (where the first subscript is a number $i = 1, 2, \ldots, 2n+4$, and the second is an element H_k of the group, $k = 1, 2, \ldots, h$). Let us use the abbreviation Q_{ij} for the "scalar product":

$$Q_{ij} = \sum_{k=1}^{h} x_{i,H_k} x_{j,H_k}.$$

Then consider the quadratic form

$$Q = Q_{12} + Q_{14} + Q_{15} + Q_{23} + Q_{24} + Q_{35} + Q_{36} + Q_{4,2n+4} + Q_{67} + Q_{78} + Q_{89} + \cdots + Q_{2n+3,2n+4} + S,$$

where S stands as an abbreviation for

$$S = \sum_{h=1}^{h} (x_{5,H_h} x_{6,H_1H_h} + x_{7,H_h} x_{8,H_2H_h} + \cdots + x_{2n+3,H_h} x_{2n+4,H_nH_h}).$$

It is easy to see that each variable x_{i,H_h} appears in Q just 3 times; hence the quadratic form Q defines a cubical graph G with $(2n + 4)h$ vertices. We give it in Figure 6 for the example of the direct product of two cyclic groups of order 2 ($h = 4$, $n = 2$), i.e. the group with the following multiplication table:

	H_1	H_2	H_3	H_4
H_1	H_4	H_3	H_2	H_1
H_2	H_3	H_4	H_1	H_2
H_3	H_2	H_1	H_4	H_3
H_4	H_1	H_2	H_3	H_4

(Of course for the construction of the graph only the first two lines are needed, as $n = 2$).

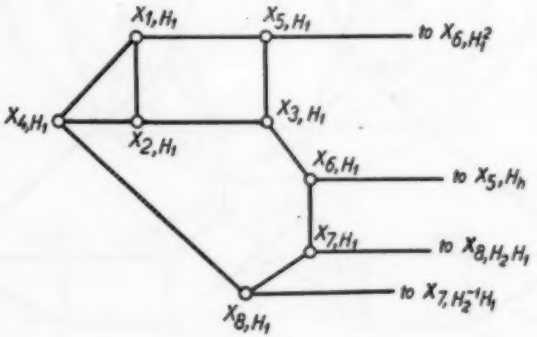

Fig. 7

For the more general case of any group generated by $n = 2$ elements we give in Figure 7 only a "corner" of the graph G, namely the vertices corresponding to the variables x_{i,H_1} (with the second subscript equal to H_1).

The proof that the graph G defined by the quadratic form Q has a group simply isomorphic to the given abstract group $\mathfrak{H}$ may be divided into two steps: firstly it has to be shown that G admits h different mappings into itself which constitute a group isomorphic to $\mathfrak{H}$; in the second place it must be proved that there are no other mappings of G into itself.

First step: It must be shown that there are h different permutations σ_1, $\sigma_2, \ldots \sigma_h$ of the variables x_{i,H_k} constituting a group simply isomorphic to $\mathfrak{H}$ and leaving the quadratic form Q unaltered. This is not difficult, as these permutations may be given explicitly by the formula

$$\sigma_m = \begin{pmatrix} x_{i,H_k} \\ x_{i,H_kH_m} \end{pmatrix}, \qquad (i = 1, 2, \ldots, 2n+4;\ k = 1, 2, \ldots, h)$$

where m runs through $1, 2, \ldots h$. It is obvious that $\sigma_1, \sigma_2, \ldots, \sigma_h$ constitute a permutation group simply isomorphic to $\mathfrak{H}$, and it is also readily shown that each σ_m leaves the quadratic form Q unaltered. Indeed it is easy to verify that each σ_m leaves unchanged each of the $(2n+6)$ quadratic forms Q_{ij} which appear in the formula given above for Q, since σ_m changes Q_{ij} into

$$\sum_{k=1}^{h} x_{i,H_kH_m} x_{j,H_kH_m} = \sum_{k'=1}^{h} x_{i,H_{k'}} x_{j,H_{k'}} = Q_{ij}$$

as with H_k also $H_kH_m = H_{k'}$ runs through the whole group $\mathfrak{H}$. Similarly it can be shown that also each of the sums $\sum_{k=1}^{h} x_{5,H_k} x_{6,H_1H_k}$, $\sum_{k=1}^{h} x_{7,H_k} x_{4,H_2H_k} \cdots$ (whose sum equals S) is left unchanged by σ_m. Let us verify this e.g. for the second sum: $\sum_{k=1}^{h} x_{7,H_k} x_{8,H_2H_k}$. It is changed by σ_m into $\sum_{k=1}^{h} x_{7,H_kH_m} x_{8,H_2H_kH_m}$, i.e. it remains unchanged, as with H_k also the product H_kH_m runs through the whole group.

Second step: It remains to be shown that *any* mapping τ of the graph G into itself coincides with one of the h permutations $\sigma_1, \sigma_2, \ldots, \sigma_h$.

For the sake of simplicity we will give this part of the proof only for the case $n = 2$, but the reader will easily see that it might be likewise given for any $n > 2$; however it would be still more tedious than for $n = 2$.

With the aid of Figure 7 (and of Figure 6, when H_1 or H_2 are elements of order 2 in the group $\mathfrak{H}$) the following types are found for the vertices x_{i,H_1} of G:

x_{1,H_1} and x_{2,H_1} . . . . . (3, 4, 5)

x_{3,H_1} . . . . . { (4, 6, 7) if H_1 is not of order 2; (4, 6, 6) if H_1 is of order 2

x_{4,H_1} . . . . . (3, 6, 7)

x_{5,H_1} . . . . . { (4, *, *) if H_1 is not of order 2; (4, 6, 8) if H_1 is of order 2

x_{6,H_1} . . . . . { (6, *, *) if H_1 is not of order 2; (6, 6, 9) if H_1 is of order 2

x_{7,H_1} . . . . . { (6, *, *) if H_2 is not of order 2; (4, 6, 8) if H_2 is of order 2

x_{8,H_1} . . . . . { (6, *, *) if H_2 is not of order 2; (4, 6, 8) if H_2 is of order 2

and the same values would hold for the other vertices x_{i,H_k} $(k = 2, 3, \ldots, h)$. (The stars stand for higher values than those given for generating elements of order 2.)

Since the only vertices of type (3, 6, 7) are $x_{4,H_1}, x_{4,H_2}, \ldots, x_{4,H_h}$, these can be only permuted among themselves by any mapping τ of the graph into itself. We must now distinguish two cases:

Case 1: τ leaves x_{4,H_1} unchanged. In this case we wish to show that $\tau = \sigma_h$ (identity). To this purpose let us consider in the first place the vertex x_{3,H_1}. (If $n > 2$ we should begin with x_{2n+4,H_1}). It must remain fixed too, as the other two neighbours of x_{4,H_1} (viz. $x_{1,H1}$ and x_{2,H_1}) have other types. Can these two neighbours of x_{4,H_1} be interchanged by τ? It is true that they have the same type (3, 4, 5); but x_{2,H_1} has a neighbour of type (4, 6, 6) or (4, 6, 7)—namely x_{3,H_1}—and x_{1,H_1} has no such neighbour. Hence x_{1,H_1} and x_{2,H_1} cannot be interchanged by τ, and therefore must be left fixed. The same will then be true of their "third neighbours" x_{3,H_1} and x_{5,H_1}, and of x_{6,H_1} as the third neighbour of x_{3,H_1}. Finally x_{7,H_1} must remain unchanged as the only common neighbour of the fixed-points x_{6,H_1} and x_{8,H_1}. (If $n > 2$ this part of the proof would be still longer, because it ought to be shown analogously that the whole "chain" $x_{6,H_1}, x_{7,H_1}, x_{8,H_1}, \ldots, x_{2n+4,H_1}$ remains unchanged).

Hence all the vertices x_{i,H_1} (with the second subscript H_1) are left fixed by τ. But x_{6,H_1} has the third neighbour x_{5,H_h} which must remain unchanged too, and by a reasoning similar to that given above it will follow that also all the vertices x_{i,H_h} (with the second subscript H_h) are left fixed by τ; the same will hold for all the vertices x_{i,H_2H_1}, since x_{7,H_1} has the third neighbour x_{8,H_2H_1}, etc. Going on in this manner until all the vertices of G are recognized as fixed, it will be possible to show that (in the case considered here) τ is the identity.

Case 2: τ maps x_{4,H_1} into some other x_{4,H_r} $(r \neq 1)$. Then the multiplication table of the group $\mathfrak{H}$ will always allow us to find a subscript s such that

$$H_s = H_1^{-1}H_r;$$

then the permutation

$$\sigma_s = \begin{pmatrix} x_{i,H_k} \\ x_{i,H_kH_s} \end{pmatrix}$$

will take x_{4,H_1} into $x_{4,H_1H_s} = x_{4,H_r}$, and σ_s^{-1}, the inverse permutation of σ_s, will change x_{4,H_r} into x_{4,H_1}. Hence the product $\tau\sigma_s^{-1}$ will be a mapping of G into itself which leaves x_{4,H_1} unchanged, and (according to the result obtained in the foregoing case 1) must be the identity: $\tau\sigma_s^{-1} = \sigma_h$. Hence $\tau = \sigma_s$.

Having thus finished the proof of Theorem 4.1, it should be remarked that in the case of some special groups fewer than $(2n + 4)h$ vertices may be needed to obtain a cubical graph whose group is simply isomorphic to a given abstract

group $\mathfrak{H}$; e.g. for the direct product of two groups of order 2 our theorem gave us the cubical graph of Figure 6 with 32 vertices, but to the same abstract group belongs also the cubical graph of Figure 8 with only 8 vertices. Other examples were already mentioned in the introduction.

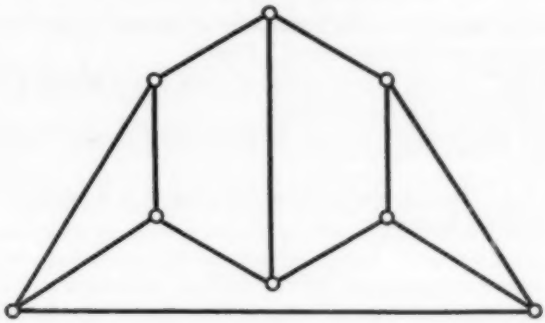

Fig. 8

A general reduction of the number of necessary vertices is however possible when we remove the condition that the graph is to be cubical.

THEOREM 4.2. *If $\mathfrak{H}$ is a non-cyclic group of order h and generated by n of its elements, one can find a graph with $2nh$ vertices whose group is simply isomorphic to $\mathfrak{H}$.* (For cyclic groups see Theorem 3.2).

This graph may be given by the following quadratic form in $2nh$ variables $x_{i,H_k}(i = 1, 2, \ldots, 2n;\ k = 1, 2, \ldots, h)$:

$$\sum_{k=1}^{h} (x_{1,H_k}x_{2,H_k} + x_{2,H_k}x_{3,H_k} + \ldots + x_{2n-1,H_k}x_{2n,H_k})$$

$$+ \sum_{k=1}^{h} (x_{1,H_k}x_{2n,H_k} + x_{2,H_k}x_{2n,H_k} + \ldots + x_{2n-2,H_k}x_{2n,H_k})$$

$$+ \sum_{\kappa<\lambda} x_{1,H_\kappa}x_{1,H_\lambda} + \sum_{k=1}^{h} (x_{1,H_k}x_{2,H_1H_k} + x_{3,H_k}x_{4,H_2H_k} + \ldots + x_{2n-1,H_k}x_{2n,H_nH_k}).$$

(The meaning of the H_k is the same as above.)

We omit the proof of Theorem 4.2, as it is similar to that of Theorem 4.1 and can be readily supplied by the reader.

As a final remark to the theorems of this section we wish to emphasize that the number of vertices we needed for the construction of a (cubical or general) graph with given abstract group of order h depends not only on h, but also on the number n of elements needed to generate the group. If we wish, however, to obtain an upper bound for the number of necessary vertices depending only on the order h of the given group, we might proceed in the following way:

Let $h = p^\alpha q^\beta r^\gamma \ldots$ (where $p, q, r, \ldots$ are distinct primes); then it can easily

be proved that it is always possible to generate a group of order h with $n \leqq \alpha + \beta + \gamma + \ldots$ elements; hence

$$2^n \leqq 2^\alpha \times 2^\beta \times 2^\gamma \times \ldots \leqq p^\alpha q^\beta r^\gamma \ldots = h,$$

and

$$n \leqq \log h / \log 2.$$

(The base of the logarithms does not matter of course; it needs only to be the same in numerator and denominator). Hence:

THEOREM 4.3. *To any abstract group of order $h > 1$ belongs a cubical graph with at most $[2h(2 + \log h/\log 2)]$ vertices.*

In the same way it would be easy to prove the following theorem for non-cubical graphs:

THEOREM 4.4. *To any abstract group of order $h > 3$ belongs a graph with at most $[2h \log h/\log 2]$ vertices.*

REFERENCES

[1] Denés König, *Theorie der endlichen und unendlichen Graphen. Kombinatorische Topologie der Streckenkomplexe.* (Leipzig, 1936). See page 5.

[2] R. Frucht, "Herstellung von Graphen mit vorgegebener abstrakter Gruppe," *Compositio Math.*, vol. 6 (1938), 239-250.

[3] I. N. Kagno, "Desargues' and Pappus' Graphs and Their Groups," *Amer. J. Math.*, vol. 69 (1947), 859-862; see footnote 2 on page 859.

[4] W. T. Tutte, "A Family of Cubical Graphs," *Proc. Cambridge Philos. Soc.*, vol. 43 (1948), 459-474.

[5] R. Frucht, "Die Gruppe des Petersenschen Graphen und der Kantensysteme der regulären Polyeder," *Comment. Math. Helv.*, vol. 9 (1937), 217-223.

[6] I. N. Kagno, "Linear Graphs of Degree $\leqq 6$ and Their Groups," *Amer. J. Math.*, vol. 68 (1946), 505-520, and vol. 69 (1947), 872.

Universidad Técnica F. Santa Maria
Valparaiso, Chile

FACTORIZATION LADDERS AND EIGENFUNCTIONS

G. F. D. DUFF

THE eigenfunctions of a boundary value problem are characterized by two quite distinct properties. They are solutions of ordinary differential equations, and they satisfy prescribed boundary conditions. It is a definite advantage to combine these two requirements into a single problem expressed by a unified formula. The use of integral equations is an example in point. The subject of this paper, namely the Schrödinger-Infeld Factorization Method, which is applicable to certain restricted Sturm-Liouville problems, is based upon another combination of the two properties. The Factorization Method prescribes a manufacturing process. From one eigenfunction we can derive another by means of operators which are constructed directly from the differential equation. Given a starting point, the operators can be applied repeatedly to build up "eigenfunction ladders" containing all the solutions of the problem. The two requirements are thus automatically fulfilled by the process of construction.

Further progress would be made by mechanizing the recursive manufacturing process in the same way that the operators mechanized the fulfilment of the two characteristic properties. We shall show that this is actually possible for a large class of problems, many of which are fundamental in Quantum Mechanics.

The operator formulae we shall treat are first order linear homogeneous differential difference equations. A systematic exposition of the properties of such equations has recently been made available through the work of Truesdell [1]. The F-equation

$$\frac{\partial}{\partial z} F(z, a) = F(z, a + 1)$$

has been made the salient feature of his treatment, and a thorough discussion of solutions $F(z, a)$ has been given. This theory provides a powerful tool for the formal manipulation of special functions. Relations of the form

$$\frac{\partial}{\partial y} f(y, a) = A(y, a)\, f(y, a) + B(y, a)\, f(y, a + 1)$$

are discussed, and a "reducibility condition" on A and B is found, which allows this equation to be transformed into the F-equation. This reduction process is the key to the present treatment of the eigenfunction problem. We shall therefore use the Factorization Method to set up a framework directly from the

Received January 10, 1949.

differential equation of Sturm-Liouville type. Then we shall show how the F-equation technique leads directly to explicit formulae for the eigenfunctions of every physical problem tractable by factorization. The complete solutions are found without reference to any theory of the special functions involved, or to the classical methods for the solution of differential equations.

1. Factorization ladders and the reducibility condition. The Factorization Method replaces the second order equation

$$u'' + r(x, m)u + \lambda u = 0, \qquad a \leq x \leq b,\ m = 0, 1, 2, \ldots \tag{1.1}$$

and its associated boundary conditions, which we shall always take as

$$u(a) = 0, \quad u(b) = 0, \quad \int_a^b u^2 dx = 1, \tag{1.2}$$

by a system of two first order equations

$$\left\{k(x, m+1) - \frac{d}{dx}\right\} u_l^m(x) = A_l^{m+1} u_l^{m+1}(x) \tag{1.3a}$$

$$\left\{k(x, m+1) + \frac{d}{dx}\right\} u_l^{m+1}(x) = A_l^{m+1} u_l^m(x) \tag{1.3b}$$

where u_l^m, u_l^{m+1} are contiguous eigenfunctions belonging to the eigenvalue $\lambda_l = L(l+1)$, $l = 0, 1, 2 \ldots$;

$$A_l^{m+1} = [L(l+1) - L(m+1)]^{\frac{1}{2}} \tag{1.4}$$

is a constant which vanishes when $m = l$, and so provides a convenient starting point. We will show that, given a normalized starting point, we can use the recurrence formulae (1, 3) to generate other eigenfunctions, a certain number of which will also be normalized.

THEOREM 1. Suppose that corresponding to $m = l$ or $l+1$ there exists a normalized eigenfunction

$$Ce^{\pm\int_{x_0}^{x} k(\nu, l+1)\, d\nu}. \tag{1.5}$$

Then for neighbouring integral values of m there exist normalized eigenfunctions given by (1.3), provided that the corresponding constants A_l^m are real and different from zero.

The proof falls naturally into three stages. First we note that the starting solution vanishes at the endpoints. Suppose that its zero of lesser order is of order $p \geq 1$. Now the manufacturing process involves operations of the type $k(x, m) \pm \dfrac{d}{dx}$ which can reduce the order of the zero at an endpoint by one at most, provided that $k(x, m)$ has no singularities more severe than the first order. We shall later verify that this is true for all the functions $k(x, m)$ which are rational in m. Then, if $|m - l| \leq p$, u_l^m also vanishes at the endpoints. If p is infinite, the ladder of eigenfunctions vanishing at the endpoints may be indefinitely long.

We see next that on the ladder so formed the normalization is preserved. Using (1.3) we have

$$A_l^{m+1}\int_a^b (u_l^{m+1})^2 dx = \int_a^b u_l^{m+1}\left[k(x, m+1) - \frac{d}{dx}\right] u_l^m dx$$

$$= \int_a^b u_l^m \left[k(x, m+1) + \frac{d}{dx}\right] u_l^{m+1} dx = A_l^{m+1}\int_a^b (u_l^m)^2 dx \tag{1.6}$$

provided that the product $u_l^m u_l^{m+1}$ vanishes at a and b. The result follows when the non-zero factor A_l^m is cancelled.

With this result it is easy to show that the ladder cannot exist if $L(l+1) - L(m) \leqslant 0$ for any value of m on the ladder. The A_l^m are then imaginary, so that if u_l^m is real, u_l^{m+1} must be pure imaginary. Unless both are identically zero, the normalization condition above would equate a positive and a negative number.

The two Corollaries which follow cover most of the particular cases we shall meet.

COROLLARY 1. If $L(m)$ is an increasing function of m for $m \geqslant 0$, then the permitted values of l and m are

$$l = 0, 1, 2, 3 \ldots$$
$$m = 0, 1 \ldots l.$$

We obtain a finite ladder of eigenfunctions $u_l^0, u_l^1 \ldots u_l^l$, which will be called an Infeld ladder [2]. At the top of each ladder we have the starting point

$$u_l^l = Ce^{\int_{x_0}^x k(\nu, l+1)d\nu}. \tag{1.7}$$

COROLLARY 2. If $L(m)$ is a decreasing function of m for $m \geqslant 0$ then the permitted values for l and m are

$$l = 0, 1, 2 \ldots$$
$$m = l, l+1, l+2 \ldots .$$

An infinite ladder is obtained for each value of l. As Schrödinger used infinite ladders in the solution of the Kepler problem we shall refer to these as Schrödinger ladders. In this case

$$u_l^l = Ce^{-\int_{x_0}^x k(\nu, l)d\nu}. \tag{1.8}$$

The solutions of (1.1) satisfying (1.2) are not necessarily the only solutions of physical interest. If the discrete spectrum function $L(m)$ has a maximum value, there may be a continuous spectrum for values of λ exceeding this value. A proof of the uniqueness of the discrete solutions here discussed can be given for the particular cases, but it involves an appeal to the indicial equation of Frobenius.

We now derive the condition that the recurrence formulae be reducible to the F-equation. Both (1.3a) and (1.3b) are of the more general form

$$\frac{d}{dx}f(x, m) = K(x, m)f(x, m) + A(m)f(x, m+1) \tag{1.9}$$

where $A(m)$ does not depend upon x. This equation is easily transformed into

$$\frac{d}{dx}\left[e^{-\int_{x_0}^{x} K(\nu,m)d\nu} f(x,m)\right] = A(m)e^{\int_{x_0}^{x}\Delta K(\nu,m)d\nu}\left[e^{-\int_{x_0}^{x} K(\nu,m+1)d\nu} f(x,m+1)\right],$$

where $\Delta K(\nu, m) = K(\nu, m+1) - K(\nu, m)$.

Suppose now that the coefficient $A(m)e^{\int_{x_0}^{x}\Delta K(\nu,m)d\nu}$ is the product of a function of x and a function of m; its two factors can be absorbed by redefining the dependent and independent variables of (1.9). Then we have

$$\log A(m) + \int_{x_0}^{x}\Delta K(\nu,m)d\nu = M(m) + \int K(x)dx.$$

By differentiation, $\Delta K(\nu, m) = K(x)$ must be independent of m. Summing this difference equation, we have

$$K(x,m) = mK(x) + K_0(x), \tag{1.10}$$

where $K(x)$ and $K_0(x)$ are arbitrary functions. We shall now show that this condition is necessary and sufficient that the recurrence formula (1.9) be reducible to the F-equation. For, when (1.10) is satisfied, and only then, may we define by the formula

$$z = \int_{x_1}^{x} e^{\int_{x_0}^{x}\Delta K(\nu,m)d\nu}dx \tag{1.11}$$

a quantity z independent of m. If also

$$F(z,m) = \left(\prod_{r=m_0}^{m-1} A(r)\right)^{-1} e^{-\int_{x_0}^{x} K(\nu,m)d\nu} f(x,m), \tag{1.12}$$

the equation (1.9) becomes

$$\frac{d}{dz}F(z,m) = F(z,m+1), \tag{1.13}$$

which is the F-equation. We have proved

THEOREM 2. The reducibility condition for the Factorization Method is that $k(x, m)$ be linear in m.

The formula we shall actually use is, of course, not (1.13), but its n-fold iterate.

THEOREM 3. Any solution $F(z, m)$ of (1.13) satisfies

$$\frac{d^n}{dz^n}F(z,m) = F(z,m+n) \qquad (n = 0, 1, 2 \ldots). \tag{1.14}$$

This quite trivial formula enables us to exhibit finite expressions for a large class of eigenfunctions.

We turn now to the analysis by which the factorizable second order equations can be enumerated. Let us begin with the two adjoint linear differential recursion formulae (1.3), which are sufficient to characterize the eigenvalue

problem completely. Eliminating either u_l^m or u_l^{m+1}, we are led to the second order differential equation in one of the two forms:

$$\text{(1.15a)}\quad \left\{k(x,m+1)+\frac{d}{dx}\right\}\left\{k(x,m+1)-\frac{d}{dx}\right\}u_l^m=\left\{L(l+1)-L(m+1)\right\}u_l^m$$

$$\text{(1.15b)}\quad \left\{k(x,m)\quad -\frac{d}{dx}\right\}\left\{k(x,m)\quad +\frac{d}{dx}\right\}u_l^m=\left\{L(l+1)-L(m)\quad\right\}u_l^m.$$

These two equations are the same, and we find in consequence the differential difference equation

$$\text{(1.16)}\quad k^2(x,m+1)-k^2(x,m)+k'(x,m+1)+k'(x,m)=L(m)-L(m+1).$$

We shall take the view that the entire Factorization Theory is implicitly contained in this fundamental equation. To a given function $k(x,m)$ corresponds a factorizable Sturm-Liouville equation if the expression formed with $k(x,m)$ according to (1.16) is independent of x. A discrete spectrum function $L(m)$ is thus determined by the same equation. The constants A_l^m appearing in the recurrence formulae are then given by (1.4).

The equation (1.16) was derived by Stevenson and Infeld [3], who have tabulated a number of solutions $k(x,m)$ with their corresponding $L(m)$. They have shown that there are no polynomial solutions in powers of m or m^{-1} of degree higher than the first. A solution such as $(-1)^m f(x)$ leads to $L(m)=0$, and is of no further interest here. If $k(x,m)$ and $L(m)$ constitute a solution of (1.16), it is easily verified that

$$\text{(1.17)}\quad \begin{array}{ll} -k(-x,m),\ L(m) & k(-x,-m),\ L(-m) \\ -k(x,-m),\ L(-m) & -ik(ix,m),\ -L(m) \end{array}$$

also constitute solutions. It is now sufficient to consider only positive values of m.

To find the solutions of (1.16), let us first assume with Stevenson and Infeld [3] that

$$\text{(1.18)}\quad k(x,m)=k_0(x)+mk_1(x).$$

Substitution of this form into (1.16), combined with the requirement that all coefficients of m in the resulting expression be constant, leads to ordinary differential equations for $k(x)$ and $K(x)$. These are

$$\text{(1.19a)}\quad k_1^2+k_1'=-a^2$$

$$\text{(1.19b)}\quad k_0k_1+k_0'=-\gamma a^2$$

where a^2 and γa^2 are independent constants. Direct solution of these equations leads to the functions[1] (a), (b), (c), (d). Employing the fourth transformation in (1.17) above, we have also (e) and (f) as real solutions of (1.16). These six functions will lead to reducible recurrence formulae.

Another trial solution for $k(x,m)$ is

$$\text{(1.20)}\quad k(x,m)=k_0(x)+mk_1(x)+m^{-1}k_{-1}(x).$$

---

[1]See Table I.

TABLE I

No.	$k(x, m)$	$L(m)$	Range (x)	Ladder Infeld—Class I Schröd.—Class II	Reducibility
a	$\alpha(m+\gamma)\cot \alpha x + \dfrac{C}{\sin \alpha x}$	$\alpha^2(m+\gamma)^2$	$\left(0, \dfrac{\pi}{\alpha}\right)$	I	Reducible
b	$\dfrac{m+\gamma}{x} + \dfrac{bx}{2}$	$-2b(m+\gamma)$	$(0, \infty)$	I $b<0$ II $b>0$	Reducible
c	ax	$-2am$	$(-\infty, \infty)$	I $a<0$ II $a>0$	Reducible
d	$Ce^{\beta x} - \beta(m+\gamma)$	$-\beta^2(m+\gamma)^2$	$(-\infty, \infty)$	II	Reducible
e	$\beta(m+\gamma)\coth \beta x + \dfrac{C}{\sinh \beta x}$	$-\beta^2(m+\gamma)^2$	$(-\infty, 0)$	II	Reducible
f	$\beta(m+\gamma)\tanh \beta x + \dfrac{C}{\cosh \beta x}$	$-\beta^2(m+\gamma)^2$	$(-\infty, \infty)$	II	Reducible
g	$\dfrac{m+\gamma}{x} - \dfrac{\nu}{m+\gamma}$	$-\dfrac{\nu^2}{(m+\gamma)^2}$	$(0, \infty)$	I	d
h	$\alpha(m+\gamma)\cot \alpha x - \dfrac{\nu}{m+\gamma}$	$\alpha^2(m+\gamma)^2 - \dfrac{\nu^2}{(m+\gamma)^2}$	$\left(0, \dfrac{\pi}{\alpha}\right)$	I	f
i	$\alpha(m+\gamma)\coth \alpha x - \dfrac{\nu}{m+\gamma}$	$-\alpha^2(m+\gamma)^2 - \dfrac{\nu^2}{(m+\gamma)^2}$	$(0, \infty)$	I	e
j	$\alpha(m+\gamma)\tanh dx - \dfrac{\nu}{m+\gamma}$	$-\alpha^2(m+\gamma)^2 - \dfrac{\nu^2}{(m+\gamma)^2}$	$(-\infty, \infty)$	II	a

Irreducible but can be transformed to

By the same procedure it is found that $k_0(x)=0$, and that $k_{-1}(x)$ is a constant; $k_1(x)$ must again satisfy the equation (1.19a). In this way (g) and (h) are determined, and (i), (j) follow from another application of (1.17). These are examples of irreducible recursion formulae. Clearly the differential equation which determines $k_1(x)$ (or $k_0(x)$) permits only first order singularities; a fact which we used in the proof of Theorem 1. We tabulate these functions, their associated spectrum functions $L(m)$, and the fundamental ranges appropriate to each.

2. Eigenfunctions on an Infeld ladder. We shall now consider the case $L(m)$ an increasing function of m, which by Corollary 1 leads to finite ladders. If $k(x, m)$ is linear in m, we have two reducible recursion formulae, and should expect to find two closed formulae for u_l^m. The two necessary starting points are easily found, but, as we shall see, one of them is sufficient to fix only the form of the eigenfunctions as transforms of certain polynomials. We shall treat first (1.3a), then (1.3b), defining functions $F_l(z, m)$ and $G_l(z, m)$ as the corresponding solutions of the F-equation. The details of the two reductions are different, so that it is advisable to set both down explicitly.

The recurrence relation (1.3a)

$$A_l^{m+1}u_l^{m+1}=\left(k(x, m+1)-\frac{d}{dx}\right)u_l^m$$

is equivalent to

$$\frac{d}{dx}\left[e^{-\int_{x_0}^{x}k(\nu,\, m+1)d\nu}u_l^m(x)\right]=-A_l^{m+1}e^{\int_{x_0}^{x}\Delta k d\nu}\left[e^{-\int_{x_0}^{x}k(\nu,\, m+2)d\nu}u_l^{m+1}(x)\right].$$

According to (1.11) we define

$$z=\int_{x_1}^{x}e^{\int_{x_0}^{x}\Delta k d\nu}dx \tag{2.1}$$

and

$$F_l(z, m)=(-1)^m\left(\prod_{r=m+1}^{l}A_l^r\right)^{-1}e^{-\int_{x_0}^{x}k(\nu,\, m+1)d\nu}u_l^m(x). \tag{2.2}$$

It is then found that

$$\frac{dF_l(z, m)}{dz}=F_l(z, m+1) \tag{2.3}$$

which is the F-equation in the variables z and m.

Because A_l^{l+1} is zero, $F_l(z, l)$ has a zero derivative, and is a constant. $F_l(z, l-1)$ is a linear function of z, and in general $F_l(z, m)$ is a polynomial of degree $l-m$ in z. The bottom of the ladder ($m=0$), is reached with $F_l(z, 0)$ a polynomial of degree l containing $l+1$ unspecified constants of integration. The complete knowledge of $F_l(z, 0)$ would enable us to determine the $F_l(z, m)$ by differentiation.

The ladder $u_l^l \ldots u_l^0$ is actually constructed with the formula (1.3b)

$$A_l^{m+1} u_l^m = \left(k(x, m+1) + \frac{d}{dx} \right) u_l^{m+1},$$

which can be written

$$\frac{d}{dx}\left[e^{\int_{x_0}^{x} k(\nu, m)\, d\nu} u_l^m(x) \right] = A_l^m e^{\int_{x_0}^{x} \Delta k\, d\nu} \left[e^{\int_{x_0}^{x} k(\nu, m-1)\, d\nu} u_l^{m-1}(x) \right].$$

As in (2.1), define $$z = \int_{x_1}^{x} e^{\int_{x_0}^{x} \Delta k\, d\nu}\, dx,$$

and

$$G_l(z, m) = \left(\prod_{r=0}^{m} A_l^r \right)^{-1} e^{\int_{x_0}^{x} k(\nu, m)\, d\nu} u_l^m(x). \tag{2.4}$$

The recurrence formula is then

$$\frac{d}{dz} G_l(z, m) = G_l(z, m-1); \tag{2.5}$$

the F-equation in the variables z and $-m$.

Note that the new independent variable z is the same in both cases. In practice, $k(x, m)$ has no singularities except at the ends of the fundamental interval, so that Δk is continuous in the open interval; z is then a monotone strictly increasing function of x in the same interval. The arbitrary constants x_0 and x_1 are to be chosen so that z will appear free of unnecessary constants.

From (1.7) it is known that

$$u_l^l = C e^{\int_{x_0}^{x} k(\nu, l+1)\, d\nu}$$

which implies

$$G_l(z, l) = C_l \left(\prod_{r=0}^{l} A_l^r \right)^{-1} e^{\int_{x_0}^{x} k(\nu, l) + k(\nu, l+1)\, d\nu} \tag{2.6}$$

$$= C_l \left(\prod_{r=0}^{l} A_l^r \right)^{-1} g_l(z)$$

where

$$g_l(z) = \exp\left[\int_{z_0}^{z} k(\nu, l) + k(\nu, l+1)\, d\nu \right] \tag{2.7}$$

is chosen to take the value 1 where $x = x_0$. With this definition we have the normalization

$$C_l = \left[\int_{z_0}^{z_1} g_l(z)\, dz \right]^{-1} \tag{2.8}$$

where (z_0, z_1) is the fundamental interval for z.

The functions $G_l(z, m)$ are the successive derivatives of $G_l(z, l)$, and can be calculated once $g_l(z)$ is known as a function of z. In practice it is easy to find the expression for $g_l(z)$, which we shall call the generating function of the lth ladder.

It is now possible to compare the expressions (2.2) and (2.4) for $u_l^m(x)$, and to find the explicit form for $F_l(z, 0)$. Thus

$$F_l(z,0) = \left(\prod_{r=1}^{l} A_l^r\right)^{-1} e^{-\int_{z_0}^{z} k(\nu,1)\,d\nu}\, u_l^0(x)$$

$$= \left(\prod_{r=l}^{l} A_l^r\right)^{-1} e^{-\int_{z_0}^{z} k(\nu,1)+k(\nu,0)\,d\nu}\, G_l(z,0) \tag{2.9}$$

$$= C_l A_l^0 \left(\prod_{r=0}^{l} A_l^r\right)^{-2} \frac{1}{g_0(z)} \frac{d^l}{dz^l}\, g_l(z).$$

Then we have

$$F_l(z,m) = C_l A_l^0 \left(\prod_{r=0}^{l} A_l^r\right)^{-2} \frac{d^m}{dz^m} \frac{1}{g_0(z)} \frac{d^l}{dz^l}\, g_l(z). \tag{2.10}$$

The closed formulae for $u_l^m(x)$ which we seek are:
from (2.2)

$$u_l^m(x) = (-1)^m \left(\prod_{r=m+1}^{l} A_l^r\right) e^{\int_{z_0}^{z} k(\nu,\,m+1)\,d\nu}\, F_l(z,m) \tag{2.11}$$

and from (2.4)

$$u_l^m(x) = \left(\prod_{r=0}^{m} A_l^r\right) e^{-\int_{z_0}^{z} k(\nu,\,m)\,d\nu}\, G_l(z,m). \tag{2.12}$$

The latter can be expressed entirely in terms of the generating function $g_l(z)$ if we make use of (2.6) and (2.7). The final result is, then:

$$u_l^m(x) = C_l \left(\prod_{r=m+1}^{l} A_l^r\right)^{-1} \frac{1}{\sqrt{g_{m-1}(z)}} \frac{d^{l-m}}{dz^{l-m}}\, g_l(z) \tag{2.13}$$

where

$$g_l(z) = \exp\left[\int_{z_0}^{z} k(\nu, l+1) + k(\nu, l)\,d\nu\right];$$

$$A_l^m = \left[L(l+1) - L(m)\right]^{\frac{1}{2}}; \text{ and } C_l = \left[\int_{z_0}^{z_1} g_l(z)\,dz\right]^{-\frac{1}{2}}.$$

The normalization of (2.13) over x is equivalent to the normalization over z of the orthogonal polynomials

$$\frac{1}{g_m(z)} \frac{d^{l-m}}{dz^{l-m}}\, g_l(z) \qquad (l = m, m+1 \ldots) \tag{2.14}$$

with weight function $g_m(z)$.

According to our programme, we have mechanized the construction of the eigenfunctions in two different ways. However, one of these is illusory, because there is no independent starting point for it. The equivalence of the two formulae for u_l^m implies that

$$F_l(z,m)g_m(z)/G_l(z,m) \tag{2.15}$$

is a constant, independent of z. This is easily verified by induction on m.

We can now apply these results to the k-functions of reducible Infeld type. Taking first

$$k(x, m) = \alpha(m + \gamma) \cot \alpha x + \frac{C}{\sin \alpha x} \qquad 0 \leq x \leq \frac{\pi}{\alpha} \tag{2.16a}$$

we find from (1.16), (2.1), (2.6) and (2.7)

$$\begin{aligned} L(m) &= \alpha^2(m + \gamma)^2 \\ r(x, m) &= -\frac{\alpha^2(m + \gamma + 1)(m + \gamma) - C^2 - 2C\alpha(m + \gamma + \tfrac{1}{2}) \cos \alpha x}{\sin^2 \alpha x} \\ \alpha z &= -\cos \alpha x \qquad -1 \leq \alpha z \leq 1 \qquad (2.17) \\ g_l(z) &= (1 - \alpha z)^{l+\gamma+\frac{1}{2}-\frac{C}{\alpha}} (1 + \alpha z)^{l+\gamma+\frac{1}{2}+\frac{C}{\alpha}} \\ F_l(z, 0) &= \text{const. } P_l(\alpha z)^{\left(l+\gamma+\frac{1}{2}-\frac{C}{\alpha},\, l+\gamma+\frac{1}{2}+\frac{C}{\alpha}\right)} \end{aligned}$$

where $P_l^{\beta,\gamma}(\alpha z)$ denotes the Jacobian polynomial of degree l [4]. When the necessary condition $\left|\frac{C}{\alpha}\right| < l + \gamma + \frac{3}{2}$ is satisfied, the normalized eigenfunctions are given by

$$\begin{aligned} u_l^m(x) = \frac{\alpha^{l-m+\frac{1}{2}}}{2^{l+\gamma+\frac{1}{2}}} &\left[\frac{(l + \gamma + 1)\,\Gamma(l + m + 2\gamma + 2)}{\Gamma\left(l + \gamma + \frac{C}{\alpha} + \frac{3}{2}\right)\Gamma\left(l + \gamma - \frac{C}{\alpha} + \frac{3}{2}\right)\Gamma(l - m + 1)}\right]^{\frac{1}{2}} \\ &+ (\sin \alpha x)^{m+\gamma+\frac{1}{2}} \left(\tan \frac{\alpha x}{2}\right)^{\frac{C}{\alpha}} P_{l-m}^{\left(m+\gamma+\frac{1}{2}+\frac{C}{\alpha},\, m+\gamma+\frac{1}{2}-\frac{C}{\alpha}\right)}(\cos \alpha x). \end{aligned} \tag{2.18}$$

Several particular cases of this formula can be noted. To obtain the spherical harmonics, set $C = 0$, $\alpha = 1$, $\gamma = 0$. The cases $C = \pm \frac{1}{2}$, $\alpha = 1$, $\gamma = -\frac{1}{2}$ are closely related to Weyl's spherical harmonics with spin, and are in fact the radial and angular eigenfunctions of the Dirac electron equations in a spherical universe. Similarly the cases $C = \pm \frac{1}{2}$, $\alpha = 1$, $\gamma = 0$ lead to the angular wave functions of an electron in a magnetic dipole field.

The second type has a semi-infinite range for x.

$$k(x, m) = \frac{m + \gamma}{x} + \frac{bx}{2} \qquad (0 \leq x < \infty) \quad b < 0. \tag{2.19}$$

The formulae

$$\begin{aligned} r(x, m) &= -\frac{(m + \gamma)(m + \gamma + 1)}{x^2} - \frac{b^2x^2}{4} + b(m + \gamma + \tfrac{1}{2}), \\ L(m) &= -2b(m + \gamma), \\ 2z &= x^2 \qquad 0 \leq z < \infty, \\ g_l(z) &= z^{l+\gamma+\frac{1}{2}} e^{bz}, \\ F_l(z, 0) &= \text{const. } L_l^{(\gamma+\frac{1}{2})}(-bz) \qquad \text{(cf. [4])}, \end{aligned} \tag{2.20}$$

follow from the definitions. For the normalized eigenfunctions we have

$$u_l^m(x) = \frac{1}{\Gamma(l-m+1)^{\frac{1}{2}}\,\Gamma(l+\gamma+\frac{3}{2})^{\frac{1}{2}}}\left(\frac{x^2}{2}\right)^{\frac{m+\gamma+1}{2}} e^{\frac{bx^2}{4}}\, L_{l-m}^{(m+\gamma+\frac{1}{2})}\left(-\frac{bx^2}{2}\right). \tag{2.21}$$

Bessel's Equation is a limiting case of each of these types, for in this case

$$k(x, m) = \frac{m-\frac{1}{2}}{x} \tag{2.22}$$

$$L(m) = 0.$$

In (2.16) set $c = 0$, $\gamma = -\frac{1}{2}$ and let a tend to zero. Similarly, set $b = 0$, $\gamma = -\frac{1}{2}$ in (2.19). The ladders break down because $L(m)$ does not vary with m. However, the Bessel equation can still be factored into a pair of adjoint recurrence formulae. In fact,

$$\left\{\frac{m+\frac{1}{2}}{x} - \frac{d}{dx}\right\} Z_m = Z_{m+1}, \tag{2.23}$$

and

$$\left\{\frac{m-\frac{1}{2}}{x} + \frac{d}{dx}\right\} Z_m = Z_{m-1}$$

differ only by the sign of m.

The third type is comparatively simple, in so far as $k(x, m)$ is independent of m. Choosing the origin so as to obtain the simplest formulas, we have

$$k(x, m) = -x \qquad -\infty \leq x \leq \infty. \tag{2.24}$$

Then

$$\begin{aligned} r(x, m) &= -2m - x^2 + 1, \\ L(m) &= 2m, \\ z &= x, \\ g_l(z) &= e^{-z^2}, \\ F_l(z, 0) &= \text{const. } H_l(z), \qquad \text{(cf.[4])}. \end{aligned} \tag{2.25}$$

The normalized eigenfunctions are

$$u_l^m(x) = \pi^{-\frac{1}{4}} 2^{-\frac{l-m}{2}}\, \Gamma(l-m+1)^{-\frac{1}{2}}\, e^{-\frac{x^2}{2}} H_{l-m}(x). \tag{2.26}$$

A factorization of this type leads to the solution of the problem of the harmonic oscillator.

In this section we have considered finite ladder problems on finite, semi-finite and infinite ranges. From the three examples it is seen how the various classical orthogonal polynomials emerge in a very natural way from the analysis when $k(x, m)$ is linear in m.

3. Eigenfunctions on a Schrödinger Ladder. We turn now to the solutions $k(x, m)$ of (1.16) corresponding to $L(m)$ a decreasing function of m. The theory of the last section needs some modification, for the roles of the two recurrence formulae are now interchanged. The formulae (2.1) to (2.5) with $(l+1)$ re-

placed by l carry over except for a constant factor in (2.2) and (2.4). For a starting point we have now, according to (1.8),

$$u_l{}^l = \bar{C} e^{-\int_{x_0}^{x} h(\nu, l)\, d\nu}$$

which implies

$$\begin{aligned} F_l(z, l) &= (-1)^l C_l e^{-\int_{x_0}^{x} h(\nu, l+1) + h(\nu, l)\, d\nu} \\ &= (-1)^l C_l g_l{}^{-1}(z). \end{aligned} \tag{3.1}$$

Thus the generating function of the infinite ladder for the eigenvalue $L(l)$ has the form of the reciprocal of the generating function of the finite ladder with eigenvalue $L(l+1)$. The normalization integral is

$$\bar{C}_l = \left[\int_{x_0}^{x_1} \frac{dz}{g_l(z)} \right]^{-\frac{1}{2}}. \tag{3.2}$$

The analogue of the final formula (2.13) is now to be found with (1.3a) and it turns out to be

$$u_l{}^m(x) = \bar{C}_l \left(\prod_{r=l+1}^{m} A_l{}^r \right)^{-1} (-1)^m \sqrt{g_{m+\frac{1}{2}}(z)}\, \frac{d^{m-l}}{dz^{m-l}} \left(\frac{1}{g_l(z)} \right). \tag{3.3}$$

The normalization of the u's again corresponds to the z normalization of the orthogonal functions

$$g_m(z) \frac{d^{m-l}}{dz^{m-l}} \frac{1}{g_l(z)} \qquad (l = 0, 1 \ldots m), \tag{3.4}$$

and weight function $\dfrac{1}{g_m(z)}$.

We shall apply these formulae to the linear k-functions for which $L(m)$ is a decreasing function of m. The first of these is the exponential solution

$$k(x, m) = Ce^{\beta x} - \beta(m + \gamma) \qquad -\infty \leq x < \infty. \tag{3.5}$$

With

$$\begin{aligned} L(m) &= -\beta^2(m + \gamma)^2 \\ r(x, m) &= 2\beta C(m + \gamma + \tfrac{1}{2})\, e^{\beta x} - C^2 e^{2\beta x}, \\ -\beta z &= e^{-\beta x}, \end{aligned}$$

$$g_l(z) = (-\beta z)^{2(l+\gamma+\frac{1}{2})} e^{-\frac{2C}{\beta z}}, \tag{3.6}$$

the eigenfunctions are given according[2] to (3.3) by

$$u_l{}^m(x) = \text{const.}\, e^{(l+\gamma)\beta x} e^{-\frac{C}{\beta} e^{\beta x}} L_{m-l}{}^{2(l+\gamma)} \left(\frac{2l}{\beta} e^{\beta x} \right). \tag{3.7}$$

We shall later apply this formula in connection with the Euclidean Kepler Problem.

The first of the hyperbolic solutions is

$$k(x, m) = \beta(m + \gamma) \coth \beta x + \frac{C}{\sinh \beta x} \qquad -\infty < x \leq 0, \tag{3.8}$$

[2]See Appendix.

which leads to

$$L(m) = -\beta^2(m+\gamma)^2$$

$$r(x,m) = -\frac{\beta^2(m+\gamma)(m+\gamma+1) + C^2 + 2\beta C(m+\gamma+\tfrac{1}{2})\cosh\beta x}{\sinh^2\beta x}$$

(3.9) $$\beta z = \cosh\beta x \qquad 1 \le \beta z < \infty$$

$$g_l(z) = (\beta z - 1)^{l+\gamma+\frac{1}{2}-\frac{C}{\beta}}(\beta z + 1)^{l+\gamma+\frac{1}{2}+\frac{C}{\beta}}.$$

The eigenfunctions are

(3.10) $$u_l^m(x) = \text{const.}\,(\sinh\beta x)^{-m-\gamma}\left(\tanh\frac{\beta x}{2}\right)^{-\frac{C}{\beta}}.$$

$$P_{m-l}^{\left(-m-\gamma-\frac{1}{2}+\frac{C}{\beta},\,-m-\gamma-\frac{1}{2}-\frac{C}{\beta}\right)}(\cosh\beta x).$$

For the normalization, $|m+\gamma| < \dfrac{C}{\beta}$ is necessary. Thus the normalized solutions end at the same "height" on each ladder.

The second hyperbolic solution is

(3.11) $$k(x,m) = \beta(m+\gamma)\tanh\beta x + \frac{C}{\cosh\beta x} \qquad -\infty < x < \infty,$$

$$L(m) = -\beta^2(m+\gamma)^2.$$

We have

$$r(x,m) = -\frac{\beta^2(m+\gamma)(m+\gamma+1) + C^2 + 2\beta C(m+\gamma+\tfrac{1}{2})\sinh\beta x}{\cosh^2\beta x},$$

(3.12) $$\beta z = \sinh\beta x,$$

$$g_l(z) = (1+i\beta z)^{l+\gamma+\frac{1}{2}+\frac{iC}{\beta}}(1+i\beta z)^{l+\gamma+\frac{1}{2}-\frac{iC}{\beta}}.$$

The eigenfunctions are

(3.13) $$u_l^m(x) = \text{const.}\,(\cosh\beta x)^{-m-\gamma}\tanh\left(\frac{\beta x}{2}+\frac{i\pi}{4}\right)^{\frac{iC}{\beta}}.$$

$$P_{m-l}^{\left(-m-\gamma-\frac{1}{2}\pm\frac{iC}{\beta}\right)}(i\sinh\beta x).$$

This last expression has only real values.

Lastly we observe that the two functions

(3.14) $$k(x,m) = \frac{m+\gamma}{x} + \frac{bx}{2}, \quad b > 0;$$

(3.15) $$= +x$$

also lead to infinite ladders. The formulae are not essentially different from the corresponding results in the last section; so we shall not include them here.

4. Eigenfunctions for the irreducible types. We turn now to the non-linear functions of m listed in section one. The first three of them occur in the radial equations of the Kepler Problem in the Euclidean, spherical, and hyperbolic spaces, respectively. For these solutions the reducibility condition of Theorem 2 is not satisfied, so that we cannot apply the method of the foregoing sections, which consists essentially of reducing to the F-equation the difference equations resulting from the factorization. However it is possible to transform the second order differential equations and to modify them in an artificial way, so that they can be factorized into reducible recurrence formulae of the types we have already treated.

The problem in the Euclidean space is the simplest of the four, and we shall treat it in some detail to illustrate the method employed. We have to solve the equation for the densities f,

$$f'' + \frac{2\nu}{x} f - \frac{(m+\gamma)(m+\gamma+1)}{x^2} f - \frac{\nu^2}{(l+\gamma)^2} f = 0. \tag{4.1}$$

The factorization of (4.1) leads to Table I, g and the method based on the linearity of $k(x, m)$ fails. Perform instead the transformation

$$f = x^{\frac{1}{2}}u;\ x = e^z$$

and obtain the equation

$$u'' + \left[2\nu e^z - \frac{\nu^2 e^{2z}}{(l+\gamma)^2} - \frac{1}{4} \right] u - (m+\gamma)(m+\gamma+1)\, u = 0. \tag{4.2}$$

This equation is quite similar to the equation of the exponential type in the preceding section. Let us introduce a new, artificial paramater "n" in such a way as to make the two equivalent. This procedure was suggested by Hull [5], who pointed out its analogy with Schrödinger's original factorization of this equation.

We find that the equation

$$u_l'' + \left[2\nu \frac{n+\gamma}{l+\gamma} e^z - \frac{\nu^2 e^{2z}}{(l+\gamma)^2} \right] u_l - (m+\gamma+\tfrac{1}{2})^2 u_l = 0 \tag{4.3}$$

is an equation of the type (3.6), leading to recurrence relations

$$\left\{ \frac{\nu e^z}{l+\gamma} - (n+\gamma+\tfrac{1}{2}) \pm \frac{d}{dz} \right\} \begin{matrix} u_{l,\,n+1}{}^m \\ u_{l,\,n}{}^m \end{matrix}$$

$$= \left[(n+\gamma+\tfrac{1}{2})^2 - (m+\gamma+\tfrac{1}{2})^2 \right]^{\frac{1}{2}} \begin{matrix} u_{l,\,n}{}^m \\ u_{l,\,n+1}{}^m \end{matrix}. \tag{4.4}$$

For a given (l, m) we obtain an infinite ladder with $n = m, m+1, m+2, \ldots$ For $n = l$, (4.4) is (4.3), so $u_{l,\,l}{}^m = u_l{}^m$. To identify (4.4) formally with (3.6) let us make the substitution

(4.5)	Exponential type	x	β	C	m	l	γ
	Kepler problem	z	1	$\dfrac{\nu}{l+\gamma}$	n	m	$\gamma - \tfrac{1}{2}$.

We can now quote the densities as

$$f_l^m = x^{\frac{1}{2}} u_{l,l}^m = C x^{m+\gamma} e^{\frac{-\nu x}{l+\gamma}} L_{l-m}^{2m+2\gamma+1}\left(\frac{2\nu x}{l+\gamma}\right). \tag{4.6}$$

To find the normalization of these functions, we recall that the normalized densities are given by a succession of operations of the form (Table I, g) on a normalized starting function like (1.7). The coefficient of the lowest power of x in a series expansion about $x = 0$ is easily worked out for this function. Comparison with the lowest coefficient in (4.6) leads to the desired normalization. As the formulas are complicated we omit them.

The spherical space [6] with quadratic form

$$ds^2 = R^2(dx^2 + \sin^2 x(d\theta^2 + \sin^2\theta d\phi^2)), \qquad x = \frac{r}{R},$$

requires that we solve the radial equation

$$s'' + (2\nu \cot x)s - \frac{(m+\gamma)(m+\gamma+1)}{\sin^2 x}\, s + (\lambda+1)s = 0. \tag{4.7}$$

The factorization of (4.7) directly yields (Table I, h). Again, let us transform by the substitution $s = \sin^{\frac{1}{2}} x\, u$; $\tan\frac{x}{2} = e^z$ and introduce an artificial parameter n in such a way that the radial equation is recovered for $n = l$. The result is the pair of recurrence formulae:

$$\left\{ \frac{\nu}{l+\gamma}\ \frac{1}{\cosh z} - (n+\gamma+\tfrac{1}{2})\tanh z \pm \frac{d}{dz} \right\} \begin{matrix} u_{l,n+1}^m \\ u_{l,n}^m \end{matrix} = \left[(n+\gamma+\tfrac{1}{2})^2 - (m+\gamma+\tfrac{1}{2})^2 \right]^{\frac{1}{2}} \begin{matrix} u_{l,n}^m \\ u_{l,n+1}^m \end{matrix}. \tag{4.8}$$

Returning to the use of x as variable, we may write the second of these as

$$\frac{d}{d(\cot x)}\left[\sin^{n+\gamma+\frac{1}{2}} x\ e^{\frac{-\nu x}{l+\gamma}} u_{l,n}^m(x) \right] = \text{const.} \sin^{n+\gamma+\frac{1}{2}} x\ e^{\frac{-\nu x}{l+\gamma}} u_{l,n+1}^m(x);$$

and with the starting point

$$u_{l,m}^m(x) = C \sin^{m+\gamma+\frac{1}{2}} x\ e^{\frac{-\nu x}{l+\gamma}}$$

we find

$$s_l^m = (\sin x)^{\frac{1}{2}} u_{l,l}^m = C \sin^{-l-\gamma} x\ e^{\frac{\nu x}{l+\gamma}} \frac{d^{l-m}}{d(\cot x)^{l-m}}\left[\sin^{2(m+\gamma+1)} x\ e^{-\frac{2\nu x}{l+\gamma}} \right]$$

$$= C \sin^{l+\gamma} x\ e^{-\frac{\nu x}{l+\gamma}} P_{l-m}^{(-l-\gamma-\frac{i\nu}{l+\gamma};\ -l-\gamma+\frac{i\nu}{l+\gamma})}(i\cot x). \tag{4.9}$$

The normalization can be effected in the same way. The formulas (4.8) are an example of (h). Allowing ν to become zero we of course recover the spherical harmonics.

The Kepler problem in the hyperbolic space can be similarly treated. We transform the usual radial equation [7] by the substitution

$$s = (\sinh x)^{\frac{1}{2}} u; \quad e^z = \tanh \frac{x}{2}$$

and introduce n. The result is the pair of recurrence formulae of the form (i).

$$(4.10) \quad \left\{ \frac{\nu}{l+\gamma} \frac{1}{\sinh z} - (n+\gamma+\tfrac{1}{2}) \coth z \pm \frac{d}{dz} \right\} \begin{matrix} u_{l,n+1}{}^{m} \\ u_{l,n}{}^{m} \end{matrix} = \left[(n+\gamma+\tfrac{1}{2})^2 - (m+\gamma+\tfrac{1}{2})^2 \right]^{\frac{1}{2}} \begin{matrix} u_{l,n}{}^{m} \\ u_{l,n+1}{}^{m} \end{matrix}.$$

Using x as variable, we find the starting point

$$u_{l,m}{}^{m}(x) = C(\sinh x)^{m+\gamma+\frac{1}{2}} e^{\frac{-\nu x}{l+\gamma}}, \qquad 0 \leq x < \infty$$

and the densities

$$(4.11) \quad s_l{}^{m} = (\sinh x)^{\frac{1}{2}} u_{l,l}{}^{m} = C(\sinh x)^{l+\gamma} e^{-\frac{\nu x}{l+\gamma}} P_{l-m}{}^{\left(-l-\gamma-\frac{\nu}{l+\gamma},\ -l-\gamma+\frac{\nu}{l+\gamma}\right)}(\coth x).$$

The normalization can be achieved only when $(l+\gamma)^2 < \nu$, so that there is a finite number of discrete energy levels in the hyperbolic space. This is just what the behaviour of $L(m)$ given by (Table I, i) predicts. For $(m+\gamma)^2 < \nu$ this function increases, but at $(m+\gamma)^2 = \nu$ it has a maximum and decreases again. The ladders corresponding to larger values of $l+\gamma$ cannot get started because $L(m)$ is a decreasing function for the initial steps down the ladder.

Our last example is a similar equation with no physical analogue, which leads to normalized eigenfunctions on Schrödinger ladders when $(l+\gamma)^2 > \nu$. We can treat this type, given by (I, j), in the same artificial way, finding the formula on an infinite ladder by means of an artificial finite ladder. Let us perform the transformation

$$s = (\cosh x)^{\frac{1}{2}} u; \quad e^z = \tan \frac{z}{2}$$

and introduce n as before. We find two relations of the first type discussed, namely (I, a):

$$(4.12) \quad \left\{ \frac{\nu}{l+\gamma} \frac{1}{\sin z} + (n+\gamma+\tfrac{1}{2}) \cot z \pm \frac{d}{dz} \right\} \begin{matrix} u_{l,n+1}{}^{m} \\ u_{l,n}{}^{m} \end{matrix} = \left[(m+\gamma+\tfrac{1}{2})^2 - (n+\gamma+\tfrac{1}{2})^2 \right]^{\frac{1}{2}} \begin{matrix} u_{l,n}{}^{m} \\ u_{l,n+1}{}^{m} \end{matrix}.$$

The starting point is

$$u_{l,m+1}{}^{m}(x) = C(\cosh x)^{-(m+\gamma+\frac{1}{2})} e^{\frac{-\nu x}{l+\gamma}}$$

corresponding to a "density" $s_l{}^{m}$ which is square integrable over $(-\infty, \infty)$ if $(l+\gamma)^2 > \nu$. The eigenfunctions can be found as functions of z with the aid of (2.18).

This last example serves to complete the pattern of the artificial correspondence of the finite and infinite ladders with the linear and non-linear k-functions. The changes of variable were all such as simply to interchange the roles of the "quantum numbers" l and m in the differential equations. The allowed values "all m less than l" become "all n greater than m," where n takes the place of l. Thus a finite ladder scheme should transform into an infinite ladder scheme, and vice versa.

We can summarize the work as follows. First we found conditions which ensure the existence of ladders of normalized eigenfunctions, and showed that two distinct classes of ladder are possible. Truesdell's reducibility condition was then enunciated. The factorizations were obtained by a method due to Stevenson and Infeld. The problems of Infeld's class led to finite ladders, while those of the class due to Schrödinger involve infinite ladders in general. We applied Truesdell's condition to the recurrence equations so found. It turned out that there are reducible and irreducible cases belonging to each class: four possibilities altogether. The next step was to work out formulae for the normalized eigenfunctions belonging to the reducible problems, and this was done for the Infeld ladders in section **2**. The reducible Schrödinger problems were treated in section **3**. Finally, in the last section we used a device which transforms each of the irreducible types into one of the known reducible problems belonging to the opposite class. An interesting artificial correspondence between the Infeld and Schrödinger ladders was thus established. In all cases treated we were able to find the normalized eigenfunctions explicitly.

Much of the elegance of the Factorization Method is due to the quite elementary character of the methods employed. We needed in addition one simple F-equation formula, and found results which are applicable to the fundamental pure problems in Quantum Mechanics.

I wish to thank Professor Infeld for his advice and encouragement throughout. Professor Truesdell very kindly read the manuscript, and his helpful criticisms are much appreciated.

Appendix

The formula used for the Laguerre function in (3.7) involves the evaluation of an nth derivative of the form

$$D_n{}^s = \frac{d^n}{dv^n}\left[v^{-s}e^{\frac{1}{v}}\right].$$

To evaluate $D_n{}^s$ consider the product $v \cdot v^{-s-1}e^{\frac{1}{v}}$ and differentiate it n times by Leibnitz' Rule. The result is

$$D_n{}^s = v\frac{d}{dv}D_{n-1}{}^{s+1} + nD_{n-1}{}^{s+1}.$$

Then

$$\frac{d}{dv}(v^n D_{n-1}{}^{s+1}) = v^{n-1}\left[v\frac{d}{dv}D_{n-1}{}^{s+1} + nD_{n-1}{}^{s+1}\right] = v^{-2}v^{n+1}D_n{}^s$$

whence

$$-\frac{d}{d\left(\frac{1}{v}\right)}\left(v^n D_{n-1}^{\,s+1}\right) = v^{n+1} D_n^{\,s}.$$

Setting $v = -\frac{1}{y}$ this is a statement that

$$(-y)^{-s-1} D_a^{\,s-a}\left(-\frac{1}{y}\right)$$

is a solution of the F-equation in the variables (y, a).
Then

$$\frac{d^n}{dy^n}\left(-\frac{1}{y} D_0^{\,s+n}\left(-\frac{1}{y}\right)\right) = \frac{d^n}{dy^n}\left((-y)^{s+n-1} e^{-y}\right)$$

$$= (-1)^{s+n-1} n!\, y^{n-1}\, e^{-y}\, L_n^{(-s-1)}(y)$$

using a well-known nth derivative formula for $L_n^{-s-1}(y)$. The result is

$$D_n^{\,s}(v) = (-1)^n n!\, v^{s+n}\, e^{\frac{1}{v}}\, L_n^{(-s-1)}\left(-\frac{1}{v}\right).$$

References

[1] C. A. Truesdell, *A Unified Theory of Special Functions* (Princeton, 1948).
[2] L. Infeld, *Phys. Rev.*, vol. 59 (1941), 737 contains a discussion of these ladders.
[3] L. Infeld and A. F. C. Stevenson. In preparation.
[4] G. Szegö, "Orthogonal Polynomials," *Amer. Math. Soc. Colloquium Publications*, vol. 23.
[5] T. E. Hull, thesis, forthcoming.
[6] E. Schrödinger, *Proc. Roy. Irish Acad.*, vol. A46 (1940) 9-16, where the Kepler problem in the spherical space was first considered.
[7] L. Infeld and A. E. Schild, *Phys. Rev.*, vol. 67 (1945) 121

University of Toronto

ON A THEOREM OF LIOUVILLE IN FIELDS OF POSITIVE CHARACTERISTIC

K. MAHLER

A classical theorem of J. Liouville[1] states that if z is a real algebraic number of degree $n \geq 2$, then there exists a constant $c > 0$ such that

$$\left| z - \frac{a}{b} \right| \geq \frac{c}{|b|^n}$$

for every pair of integers a, b with $b \neq 0$.

This theorem has an analogue in function fields. Let k be an arbitrary field, x an indeterminate, $k[x]$ the ring of all polynomials in x with coefficients in k, $k(x)$ the field of all rational functions in x with coefficients in k, and $k<x>$ the field of all formal series

$$z = a_f x^f + a_{f-1} x^{f-1} + a_{f-2} x^{f-2} + \dots$$

in x where the coefficients $a_f, a_{f-1}, a_{f-2}, \dots$ are in k. Thus $k(x)$ is the quotient field of $k[x]$ and a subfield of $k<x>$.

A valuation $|z|$ in $k<x>$ is now defined by putting $|0| = 0$; but $|z| = e^f$ if $z = a_f x^f + a_{f-1} x^{f-1} + a_{f-2} x^{f-2} + \dots$ and $a_f \neq 0$. If z lies in $k[x]$, then $\log |z|$ is simply the degree of z.

With this notation, the analogue to Liouville's theorem states:

THEOREM 1. *If the element z of $k<x>$ is algebraic of degree $n \geq 2$ over $k(x)$, then there exists a constant $c > 0$ such that*

$$\left| z - \frac{a}{b} \right| \geq \frac{c}{|b|^n}$$

for all pairs of elements a and $b \neq 0$ of $k[x]$.

Proof. Denote by

$$f(y) = a_0 y^n + a_1 y^{n-1} + \dots + a_n, \qquad \text{where } a_0 \neq 0,$$

a polynomial in y with coefficients in $k[x]$ which is irreducible over $k(x)$ and vanishes for $y = z$; further put

$$g(y) = a_0 y^{n-1} + (a_0 z + a_1) y^{n-2} + (a_0 z^2 + a_1 z + a_2) y^{n-3} + \dots + (a_0 z^{n-1} + a_1 z^{n-2} + \dots + a_{n-1}).$$

Received April 28, 1949.

[1] *C.R. Acad. Sci. Paris*, vol. 18 (1844), 883-885, 910-911.

Then

$$\frac{f(y)}{y-z} = \frac{f(y)-f(z)}{y-z} = g(y)$$

identically in y, and therefore

$$y - z = \frac{f(y)}{g(y)}.$$

Put

$$\max(|a_0|, |a_1|, \ldots, |a_n|) = c_1, \quad \max(1, |z|) = c_2$$

and take

$$y = \frac{a}{b}$$

where a and $b \neq 0$ are in $k[x]$.

If

$$\left|\frac{a}{b}\right| > c_2 = |z|,$$

then

$$\left|z - \frac{a}{b}\right| = \left|\frac{a}{b}\right| > c_2 \geq \frac{c_2}{|b|^n}, \qquad \text{since } |b| \geq 1. \tag{1}$$

Next let

$$\left|\frac{a}{b}\right| \leq c_2,$$

so that

$$\left|g\left(\frac{a}{b}\right)\right| \leq c_1 c_2^{n-1}.$$

The expression

$$b^n f\left(\frac{a}{b}\right) = a_0 a^n + a_1 a^{n-1} b + \ldots + a_n b^n$$

lies in $k[x]$ and does not vanish since $f(y)$ is irreducible and at least of the second degree. Therefore

$$\left|b^n f\left(\frac{a}{b}\right)\right| \geq 1, \quad \left|f\left(\frac{a}{b}\right)\right| \geq |b|^{-n},$$

whence

$$\left|z - \frac{a}{b}\right| = \left|\frac{f\left(\frac{a}{b}\right)}{g\left(\frac{a}{b}\right)}\right| \geq \frac{1}{c_1 c_2^{n-1} |b|^n}. \tag{2}$$

If we now put

$$c = \min\left(c_2, \frac{1}{c_1 c_2^{n-1}}\right),$$

then the assertion of the theorem is contained in (1) and (2).

In the case of a real algebraic number of degree $n \geq 3$, Liouville's theorem is not the best-possible, and it was first improved by A. Thue,[2] who showed that, for every $\epsilon > 0$, there is a constant $c(\epsilon) > 0$ such that

$$\left| z - \frac{a}{b} \right| \geq \frac{c(\epsilon)}{|b|^{\frac{n}{2}+1+\epsilon}}$$

for all pairs of integers a and $b \neq 0$. Still better inequalities were given by C. L. Siegel[3] and F. J. Dyson.[4] A similar improvement is possible in the case of the analogue of Liouville's theorem for algebraic functions, if the constant field k is the field of all complex numbers, or, more generally, any field of characteristic 0, as was proved by B. P. Gill.[5]

It is then of some interest to note that *the analogue of Liouville's theorem for algebraic functions cannot be improved if the ground field k is of characteristic p where p is a positive prime number.* Indeed, the following result holds.

THEOREM 2. *Let k be any field of characteristic p, x an indeterminate, and z the element*

$$z = x^{-1} + x^{-p} + x^{-p^2} + x^{-p^3} + \dots$$

of $k<x>$. Then z is of exact degree p over $k(x)$, and there exists an infinite sequence of pairs of elements a_n and $b_n \neq 0$ of $k[x]$ such that

$$\left| z - \frac{a_n}{b_n} \right| = |b_n|^{-p}, \quad \lim_{n \to \infty} |b_n| = \infty.$$

Proof. If $a, b, c, \dots$ are elements of $k<x>$, then

$$(a + b + c + \dots)^p = a^p + b^p + c^p + \dots,$$

by a well-known property of fields of characteristic p. Hence, in particular,

$$z = x^{-1} + (x^{-p} + x^{-p^2} + x^{-p^3} + \dots) = x^{-1} + (x^{-1} + x^{-p} + x^{-p^2} + \dots)^p$$

and so z is a root of the algebraic equation[6]

$$z^p - z + x^{-1} = 0 \tag{3}$$

of degree p over $k(x)$.

Put, for $n = 1, 2, 3, \dots$,

$$a_n = x^{p^{n-1}}(x^{-1} + x^{-p} + \dots + x^{-p^{n-1}}), \quad b_n = x^{p^{n-1}}$$

---

[2] *Norske Vid. Selsk. Scr.* (1908), Nr. 7.
[3] *Math. Zeit.*, vol. 10 (1921), 173-213.
[4] *Acta Math.*, vol. 79 (1947), 225-240.
[5] *Ann. of Math.* (2) 31 (1930), 207-218.
[6] I am indebted to E. Artin for the remark that z is algebraic if k is of characteristic p. If k is of characteristic 0, then z is, of course, transcendental over $k(x)$.

so that

$$|b_n| = e^{p^n-1}, \text{ and } \left|z - \frac{a_n}{b_n}\right| = |x^{-p^n} + x^{-p^{n+1}} + \ldots| = e^{-p^n} = |b_n|^{-p}.$$

The assertion will therefore be proved if we can show that z is of exact degree p. But, by Theorem 1, z cannot be of lower degree than p, unless it is of degree 1 and lies in $k(x)$. Suppose then that

$$z = \frac{A}{B},$$

where A and $B \neq 0$ are elements of $k[x]$. Since the fractions a_n/b_n are all different,

$$\frac{a_n}{b_n} \neq z, \; Ab_n - a_nB \neq 0, \; |Ab_n - a_nB| \geq 1,$$

for all sufficiently large n. But then

$$|b_n|^{-p} = \left|z - \frac{a_n}{b_n}\right| = \left|\frac{A}{B} - \frac{a_n}{b_n}\right| = \left|\frac{Ab_n - a_nB}{Bb_n}\right| \geq \frac{1}{|B|\,|b_n|},$$

whence

$$|B| \geq |b_n|^{p-1},$$

contrary to the fact that

$$\lim_{n\to\infty} |b_n| = \infty.$$

It would be of interest to investigate whether the analogue of Liouville's theorem remains still the best-possible for elements $k\langle x\rangle$ not in $k(x)$ which are of a degree *less than* p over $k(x)$.

Institute for Advanced Study,
Princeton, N.J.

Authoritative Mathematics Books

DIFFERENTIAL AND INTEGRAL CALCULUS: Vols. I & II

By R. Courant, Professor of Mathematics, New York University. With its first publication in 1934, this book put into printed form what was already being taught in lecture courses: the simultaneous treatment of differential calculus and integral calculus.
Volume I deals mainly with the integral and differential calculus for functions of one variable. Second edition, tenth printing, 1946, $6.00. Volume II deals mainly with functions of several variables. Ninth printing, 1945, $10.00.

THEORY AND APPLICATION OF INFINITE SERIES

By Konrad Knopp, Professor of Mathematics, University of Tübingen. Here is an introduction to the theory of real numbers, a fairly extensive account of the theory of sequences and, finally, the actual theory of infinite series. Intended for both the student attending lectures and for private study. Fourth printing, 1948, $11.50.

THE ABSOLUTE DIFFERENTIAL CALCULUS

By Tullio Levi-Civita, Professor of Rational Mechanics, University of Rome. A complete translation of the author's Italian text, and of two new chapters, specially written by him. These chapters exhibit the fundamental principles of Einstein's General Theory of Relativity as an application of the Absolute Calculus. Fourth printing, 1947, $8.00.

APPLIED BESSEL FUNCTIONS

By F. E. Relton, Professor of Mathematics, Faculty of Engineering, Egyptian University, Cairo. This book is definitely mathematical and is addressed to technicians. It is based on lectures given to graduates in physics, soil mechanics, and the various branches of civil, mechanical and electrical engineering. They had found that their researches were being impeded by their inability to handle Bessel functions. 1946, $5.75.

THE CALCULUS OF OBSERVATIONS

By Sir Edmund Whittaker, Professor of Mathematics and G. Robinson, former lecturer in mathematics, both of the University of Edinburgh. Deals with the mathematical problems which arise in dealing with numerical data. An important book for astronomers, meteorologists, physicists, engineers, naval architects, actuaries, biometricians and statisticians, as well as pure mathematicians. Eleventh printing, 1948, $9.00.

AN INTRODUCTION TO THE THEORY OF STATISTICS

By G. Udny Yule, Cambridge University, and M. G. Kendall, statistician to the Chamber of Shipping, United Kingdom. A systematic introductory course on statistical methods, suited to those who possess only a limited knowledge of mathematics. Planned not only for those interested in economic and vital statistics, but also for biologists and students of the other sciences in which statistical methods are employed. Thirteenth edition, revised, 1946, $7.25.

On account of recent devaluation, the above prices are subject to change.

The Ryerson Press ***Publishers, Toronto***